(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－43152
（P2001－43152A）
(43)公開日　平成13年２月16日(2001.2.16)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
G06F	13/00	351	G06F	13/00	351G 5B089
					351N 5K030
H04L	12/24		H04L	11/08	9A001
	12/26			11/20	101B
	12/54				

審査請求　未請求　請求項の数15　ＯＬ　（全 24 頁）　最終頁に続く

(21)出願番号　特願平11－213605

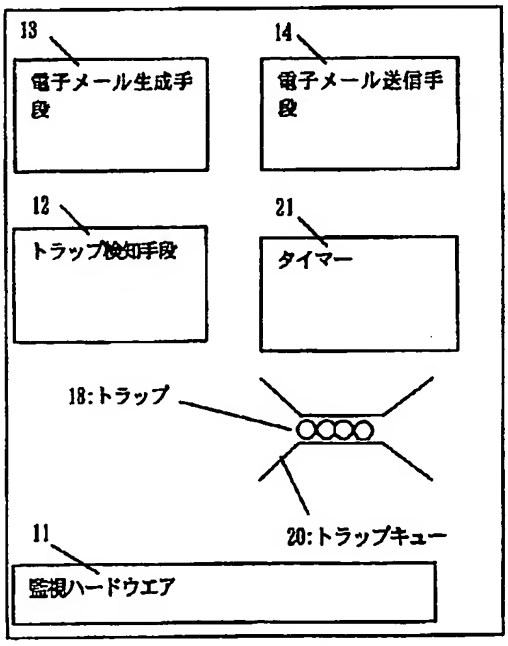
(22)出願日　平成11年７月28日(1999.7.28)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　五十嵐　政志
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　鎗川　達也
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100099461
弁理士　溝井　章司　（外２名）

最終頁に続く

(54)【発明の名称】　障害通知方式

(57)【要約】
【課題】　障害を電子メールで通知する際にいくつかのトラップをまとめる事により送信する電子メールの数を減らし通信トラフィックを削減する。
【解決手段】　トラップ検知手段１２は、監視ハードウエア１１からトラップを受信した際にタイマー２１が満了するまでの時間に受信した複数のトラップをトラップキュー２０に溜めておき、タイマー２１が満了したタイミングで、電子メール生成手段１３によりトラップの内容を電子メールの本文に示す内容で作成し、電子メール送信手段１４により、管理ＰＣにメールを送信する。



実施の形態１の構成図

1

【特許請求の範囲】

【請求項１】　障害の発生を電子メールで通知する障害通知方式において、

コンピュータの状態を監視して監視した状態を示す状態情報を保持するとともに障害検出時に状態情報をトラップとして発生させる監視ハードウェアと、

上記監視ハードウェアが障害検出時に発生させるトラップを受信してトラップの発生を検知するトラップ検知手段と、

上記トラップ検知手段が受信した１つ以上のトラップをキューイングするトラップキューと、

上記トラップキューにキューイングされた１つ以上のトラップを含む電子メールを作成する電子メール生成手段と、

上記電子メール生成手段が作成した電子メールを送信する電子メール送信手段とを備えたことを特徴とする障害通知方式。

【請求項２】　上記障害通知方式は、さらに、上記トラップ検知手段がトラップを受信してから上記電子メール送信手段が電子メールを送信するまでの猶予時間として所定の時間を計測するタイマーを備え、

上記トラップキューは、上記タイマーが計測する所定の時間が経過するまで上記トラップ検知手段が受信した１つ以上のトラップをキューイングすることを特徴とする請求項１に記載の障害通知方式。

【請求項３】　上記トラップキューは、所定のトラップを発生させた障害の後処理の完了するまでの間に上記トラップ検知手段が受信する１つ以上のトラップをキューイングすることを特徴とする請求項１に記載の障害通知方式。

【請求項４】　上記障害通知方式は、さらに、上記タイマーが計測する所定の時間の値を、前回のトラップ発生から今回のトラップ発生までの経過時間に対応させて動的に決定するタイマー値決定手段を備えたことを特徴とする請求項２に記載の障害通知方式。

【請求項５】　上記障害通知方式は、さらに、上記トラップ検知手段が受信したトラップの回数を数えるカウンタを備え、上記トラップキューは上記カウンタの値が所定の上限値に達するまで上記トラップ検知手段が受信したトラップをキューイングすることを特徴とする請求項１に記載の障害通知方式。

【請求項６】　上記障害通知方式は、さらに、上記トラップ検知手段がトラップを受信してから上記電子メール送信手段が電子メールを送信するまでの猶予時間として所定の時間を計測するタイマーと上記トラップ検知手段が受信したトラップの回数を数えるカウンタとを備え、

上記トラップキューは、上記タイマーが計測する所定の時間が経過するか、または、上記カウンタの値が所定の上限値に達するまでのいずれか一方を満足するまで、上記トラップ検知手段が受信した１つ以上のトラップをキューイングすることを特徴とする請求項１に記載の障害通知方式。

2

【請求項７】　上記障害通知方式は、トラップの種類毎に重み付けされた値を予め保持し、トラップが発生する度に重み付けされた値を加算して合計値を算出し、算出した合計値が所定の障害合計値に達するまで上記トラップ検知手段が受信したトラップを上記トラップキューにキューイングさせる障害値加算手段を備えたことを特徴とする請求項１に記載の障害通知方式。

【請求項８】　上記障害通知方式は、複数の電子メール送信先を設定するとともに、設定された電子メール送信先毎に上記障害合計値を異ならせて設定可能な送信先テーブルを備え、上記トラップ検知手段は上記送信先テーブルを参照して、電子メール送信先毎に対応する障害合計値に達する毎に、電子メールを作成、送信させることを特徴とする請求項７に記載の障害通知方式。

【請求項９】　上記障害通知方式は、コンピュータが短い時間内に停止する可能性がある重障害に対応するトラップを予め登録する重障害トラップテーブルを備え、上記トラップ検知手段は受信したトラップが上記重障害トラップテーブルに登録されている場合に、電子メールを作成、送信させることを特徴とする請求項１から８いずれかに記載の障害通知方式。

【請求項１０】　上記障害通知方式は、電子メールの送信先毎に送信するトラップを登録する送信トラップ登録テーブルと上記送信トラップ登録テーブルと電子メールの送信先との対応を定義する送信トラップ対応テーブルとを備えるとともに、

上記送信トラップ対応テーブルと上記送信トラップ登録テーブルとを参照して、電子メールの送信先毎に送信するトラップを選択して電子メール生成手段に電子メールを作成させるトラップ選別手段を備えたことを特徴とする請求項１～９いずれかに記載の障害通知方式。

【請求項１１】　障害の発生を電子メールで通知する障害通知方式において、

コンピュータの状態を監視して監視した状態を示す状態情報を保持するとともに障害検出時に状態情報をトラップとして発生させる監視ハードウェアと、

上記監視ハードウェアが障害検出時に発生させるトラップを受信してトラップの発生を検知するトラップ検知手段と、

上記トラップ検知手段が受信した１つ以上のトラップをキューイングするトラップキューと、

上記トラップキューにキューイングされた１つ以上のトラップを含む電子メールを作成する電子メール生成手段と、

上記電子メール生成手段が作成した電子メールを送信する電子メール送信手段と、

上記トラップ検知手段が検知した１つのトラップの発生が一定の時間間隔以内に起こる状態が一定時間継続した

トラップ頻発状態を検出するトラップ頻発状態検出手段とを備え、
上記トラップ検知手段は、上記トラップ頻発状態検出手段がトラップ頻発状態を検出した際に、電子メールによる障害通知を一時停止するとともに、障害通知を一時停止したことを電子メールで監視者に伝えることを特徴とする障害通知方式。
【請求項１２】　上記障害通知方式は、さらに、該トラップが発生しない状態が一定時間継続したことを検出するトラップ停止状態検出手段を備え、
上記トラップ検知手段は、上記トラップ停止状態検出手段がトラップ停止状態を検出した際に、電子メールによる障害通知を再開するとともに、障害通知を再開したことを電子メールで監視者に伝えることを特徴とする請求項１１に記載の障害通知方式。
【請求項１３】　上記障害通知方式は、さらに、頻発する可能性のある障害に対応するトラップを１つ以上記憶する頻発トラップ記憶手段を備え、
上記トラップ頻発状態検出手段は、上記頻発トラップ記憶手段が記憶するトラップのうちいずれか１つのトラップに関して、トラップ頻発状態を検出するとともに、
上記障害通知方式は、上記トラップ頻発状態が検出されたトラップに関して、電子メールによる障害通知を一時停止し、障害通知を一時停止したことを電子メールで監視者に伝えることを特徴とする請求項１１に記載の障害通知方式。
【請求項１４】　上記障害通知方式は、互いに関連する第１と第２のトラップの対と、上記第１と第２のトラップの対が連続して発生することが予想される所定の時間とを対応させて記憶するトラップ対記憶手段を備え、
上記トラップ検知手段は、上記トラップ対記憶手段を参照して、上記第１のトラップの発生を検知すると、上記所定の時間の経過、及び上記第２のトラップの発生のいずれかを待って、上記電子メール生成手段に対して電子メールを作成させ、作成した電子メールを上記電子メール送信手段により送信させることを特徴とする請求項１に記載の障害通知方式。
【請求項１５】　上記第１のトラップは障害の発生を示す障害トラップであり、上記第２のトラップは該障害トラップに対応して自動的に発生する修復トラップであり、上記所定の時間は上記障害トラップに対して上記修復トラップの発生が期待される時間であって、
上記トラップ検知手段は、上記トラップ対記憶手段を参照して、上記第１のトラップの発生を検知すると、上記所定の時間の経過を待って、修復トラップが来ない場合に上記電子メール生成手段に対して電子メールを作成させ、作成した電子メールを上記電子メール送信手段により送信させることを特徴とする請求項１４に記載の障害通知方式。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、例えば、ネットワークに接続されたコンピュータの障害監視に関するものである。また、例えば、障害の通知に電子メールを用いる障害通知方式に関するものである。
【０００２】
【従来の技術】図２９は、従来からある、電子メールによる障害通知方式を示す図である。図において、９ａは監視される対象のコンピュータ（監視対象コンピュータ）であり、障害を自身で検出し電子メールで監視者に通知する。コンピュータ９ａは、コンピュータ自身の状態を監視し状態情報を保持する監視ハードウェア９１と、監視ハードウェア９１が障害検出時に発生するトラップを受けるトラップ検知手段９２と、トラップが示す障害情報を含む電子メールを作成する電子メール生成手段９３と、作成した電子メールを送信する電子メール送信手段９４を有する。コンピュータ９ａより送信された電子メールは監視者の管理ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）３ａに送られる。２ａ，２ｂは電子メールがコンピュータ１ａから管理ＰＣ３ａに送られるまでに経由するメールサーバである。４ａ、４ｂは各々コンピュータ１ａ、管理ＰＣ３ａの設置場所に敷設されたＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、４ｃはそれらＬＡＮ同士を接続するＬＡＮまたはＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）またはＩｎｔｅｒｎｅｔである。
【０００３】ここで、「監視ハードウエア」とは、ハードウエアやソフトウエアの障害を監視するコンピュータ本体とは独立したハードウエアであり、監視対象のソフトウエアやハードウエアの現在の状況に対応する変数を持ち、変数は「監視ハードウエア」内部の不揮発性のメモリに保持される。また「トラップ」とは、障害が発生した場合に監視ハードウエアから送られる、ハードウエアやソフトウエアの障害箇所を特定するための情報の事であり、「監視ハードウエア」が持つ変数のアドレスと値を含むデータから構成される。
【０００４】次に、動作について説明する。コンピュータ９ａの監視ハードウェア９１が障害を検出すると、トラップ検知手段９２に障害を示す情報であるトラップを送る。トラップ検知手段９２はトラップを受け取ると電子メール生成手段９３を呼んでトラップの内容を電子メールの形式にして、電子メールを作成し、さらに電子メール送信手段９４を呼んで、今、電子メール生成手段９３が作成した電子メールを管理ＰＣ３ａに送信する。
【０００５】ここで、トラップ検知手段９２はトラップが発生する度に上述の動作を行う。従ってトラップの数と同じ数だけ電子メールが作成され、送信されることになる。コンピュータにある一つの障害が発生した場合、その事象に対応するトラップの数が一つであるとは限らず、一つの障害に対し複数の電子メールが送られる場合

もある。

【０００６】

【発明が解決しようとする課題】従来の、電子メールによる障害通知方式は、以上のように構成されていたので、一つの事象に対して比較的短時間の間に複数のトラップが発生した場合、個々のトラップに対応して電子メールが送られるため、監視者は障害の全貌を掴むために、複数の電子メールを見る必要があるという問題があった。

【０００７】また、電子メールは送信した順番に監視者に着信するとは限らず、特に送信間隔が短い場合は着信順序が狂う可能性が高い。このため、監視者が障害の全貌を掴むために重要となる、トラップの発生順序を特定することが困難となる問題があった。

【０００８】また、コンピュータで異常状態が継続し、トラップが頻発あるいは連続発生した際、その都度、発生したトラップの数だけ、電子メールが送られ、メールサーバ、ネットワークに余計な負荷をかけてしまう問題があった。

【０００９】この発明は、例えば、上記のような課題を解決するためになされたもので、複数のトラップが一つの電子メールにより送られ、監視者が障害の全貌を掴むのに複数の電子メールを見る必要が無いような障害通知方式を得ることを目的としている。また、例えば、電子メールに含まれるトラップの順序関係が一目瞭然で、監視者は容易にトラップの順序関係を知ることができる障害通知方式を得ることを目的としている。また、例えば、トラップ頻発および連続発生にてメールサーバ、ネットワークに余計な負荷をかけることのない、電子メールによる障害通知方式を得ることを目的とする。

【００１０】

【課題を解決するための手段】この発明の障害通知方式は、障害の発生を電子メールで通知する障害通知方式において、コンピュータの状態を監視して監視した状態を示す状態情報を保持するとともに障害検出時に状態情報をトラップとして発生させる監視ハードウェアと、上記監視ハードウェアが障害検出時に発生させるトラップを受信してトラップの発生を検知するトラップ検知手段と、上記トラップ検知手段が受信した１つ以上のトラップをキューイングするトラップキューと、上記トラップキューにキューイングされた１つ以上のトラップを含む電子メールを作成する電子メール生成手段と、上記電子メール生成手段が作成した電子メールを送信する電子メール送信手段とを備えたことを特徴とする。

【００１１】上記障害通知方式は、さらに、上記トラップ検知手段がトラップを受信してから上記電子メール送信手段が電子メールを送信するまでの猶予時間として所定の時間を計測するタイマーを備え、上記トラップキューは、上記タイマーが計測する所定の時間が経過するまで上記トラップ検知手段が受信した１つ以上のトラップをキューイングすることを特徴とする。

【００１２】上記トラップキューは、所定のトラップを発生させた障害の後処理の完了するまでの間に上記トラップ検知手段が受信する１つ以上のトラップをキューイングすることを特徴とする。

【００１３】上記障害通知方式は、さらに、上記タイマーが計測する所定の時間の値を、前回のトラップ発生から今回のトラップ発生までの経過時間に対応させて動的に決定するタイマー値決定手段を備えたことを特徴とする。

【００１４】上記障害通知方式は、さらに、上記トラップ検知手段が受信したトラップの回数を数えるカウンタを備え、上記トラップキューは上記カウンタの値が所定の上限値に達するまで上記トラップ検知手段が受信したトラップをキューイングすることを特徴とする。

【００１５】上記障害通知方式は、さらに、上記トラップ検知手段がトラップを受信してから上記電子メール送信手段が電子メールを送信するまでの猶予時間として所定の時間を計測するタイマーと上記トラップ検知手段が受信したトラップの回数を数えるカウンタとを備え、上記トラップキューは、上記タイマーが計測する所定の時間が経過するか、または、上記カウンタの値が所定の上限値に達するまでのいずれか一方を満足するまで、上記トラップ検知手段が受信した１つ以上のトラップをキューイングすることを特徴とする。

【００１６】上記障害通知方式は、トラップの種類毎に重み付けされた値を予め保持し、トラップが発生する度に重み付けされた値を加算して合計値を算出し、算出した合計値が所定の障害合計値に達するまで上記トラップ検知手段が受信したトラップを上記トラップキューにキューイングさせる障害値加算手段を備えたことを特徴とする。

【００１７】上記障害通知方式は、複数の電子メール送信先を設定するとともに、設定された電子メール送信先毎に上記障害合計値を異ならせて設定可能な送信先テーブルを備え、上記トラップ検知手段は上記送信先テーブルを参照して、電子メール送信先毎に対応する障害合計値に達する毎に、電子メールを作成、送信させることを特徴とする。

【００１８】上記障害通知方式は、コンピュータが短い時間内に停止する可能性がある重障害に対応するトラップを予め登録する重障害トラップテーブルを備え、上記トラップ検知手段は受信したトラップが上記重障害トラップテーブルに登録されている場合に、電子メールを作成、送信させることを特徴とする。

【００１９】上記障害通知方式は、電子メールの送信先毎に送信するトラップを登録する送信トラップ登録テーブルと上記送信トラップ登録テーブルと電子メールの送信先との対応を定義する送信トラップ対応テーブルとを備えるとともに、上記送信トラップ対応テーブルと上記

送信トラップ登録テーブルとを参照して、電子メールの送信先毎に送信するトラップを選択して電子メール生成手段に電子メールを作成させるトラップ選別手段を備えたことを特徴とする。

【００２０】障害の発生を電子メールで通知する障害通知方式において、コンピュータの状態を監視して監視した状態を示す状態情報を保持するとともに障害検出時に状態情報をトラップとして発生させる監視ハードウェアと、上記監視ハードウェアが障害検出時に発生させるトラップを受信してトラップの発生を検知するトラップ検知手段と、上記トラップ検知手段が受信した１つ以上のトラップをキューイングするトラップキューと、上記トラップキューにキューイングされた１つ以上のトラップを含む電子メールを作成する電子メール生成手段と、上記電子メール生成手段が作成した電子メールを送信する電子メール送信手段と、上記トラップ検知手段が検知した１つのトラップの発生が一定の時間間隔以内に起こる状態が一定時間継続したトラップ頻発状態を検出するトラップ頻発状態検出手段とを備え、上記トラップ検知手段は、上記トラップ頻発状態検出手段がトラップ頻発状態を検出した際に、電子メールによる障害通知を一時停止するとともに、障害通知を一時停止したことを電子メールで監視者に伝えることを特徴とする。

【００２１】上記障害通知方式は、さらに、該トラップが発生しない状態が一定時間継続したことを検出するトラップ停止状態検出手段を備え、上記トラップ検知手段は、上記トラップ停止状態検出手段がトラップ停止状態を検出した際に、電子メールによる障害通知を再開するとともに、障害通知を再開したことを電子メールで監視者に伝えることを特徴とする。

【００２２】上記障害通知方式は、さらに、頻発する可能性のある障害に対応するトラップを１つ以上記憶する頻発トラップ記憶手段を備え、上記トラップ頻発状態検出手段は、上記頻発トラップ記憶手段が記憶するトラップのうちいずれか１つのトラップに関して、トラップ頻発状態を検出するとともに、上記障害通知方式は、上記トラップ頻発状態が検出されたトラップに関して、電子メールによる障害通知を一時停止し、障害通知を一時停止したことを電子メールで監視者に伝えることを特徴とする。

【００２３】上記障害通知方式は、互いに関連する第１と第２のトラップの対と、上記第１と第２のトラップの対が連続して発生することが予想される所定の時間とを対応させて記憶するトラップ対記憶手段を備え、上記トラップ検知手段は、上記トラップ対記憶手段を参照して、上記第１のトラップの発生を検知すると、上記所定の時間の経過、及び上記第２のトラップの発生のいずれかを待って、上記電子メール生成手段に対して電子メールを作成させ、作成した電子メールを上記電子メール送信手段により送信させることを特徴とする。

【００２４】上記第１のトラップは障害の発生を示す障害トラップであり、上記第２のトラップは該障害トラップに対応して自動的に発生する修復トラップであり、上記所定の時間は上記障害トラップに対して上記修復トラップの発生が期待される時間であって、上記トラップ検知手段は、上記トラップ対記憶手段を参照して、上記第１のトラップの発生を検知すると、上記所定の時間の経過を待って、修復トラップが来ない場合に上記電子メール生成手段に対して電子メールを作成させ、作成した電子メールを上記電子メール送信手段により送信させることを特徴とする。

【００２５】

【発明の実施の形態】以下、この発明の実施の形態を説明する。

実施の形態１．この実施の形態、および以降の実施の形態における、システム全体の構成は、従来の図２９に示す構成と同じである。この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、電子メールを作成、送信するまでの猶予時間を与えるタイマーと、猶予時間内に受信したトラップをキューイングするトラップキューとをコンピュータ上に備えたものである。以下に、図を用いて説明する。

【００２６】図１は、実施の形態１によるコンピュータの構成を示す図である。図１においては、コンピュータの状態を監視し、状態情報を保持する監視ハードウエア１１と、監視ハードウエアからのトラップを受信するトラップ検知手段１２と、受信したトラップを元に電子メールを作成する電子メール生成手段１３と、作成した電子メールを監視者に送信する電子メール送信手段１４は、従来の図２９に示す構成の監視ハードウェア９１～電子メール送信手段９４にそれぞれ相当する。

【００２７】前述したように、「監視ハードウエア」とは、ハードウエアやソフトウエアの障害を監視するハードウエアであり、コンピュータ本体とは独立したハードウェアである。「監視ハードウエア」は、監視対象のソフトウエアやハードウエアの現在の状況に対応する変数を持つ。具体的には、監視情報を「変数アドレスと値」という形式で「監視ハードウエア」内部の不揮発性のメモリに保持している。このように、不揮発性メモリ上に保持された「変数アドレスと値」情報そのものを状態情報と呼ぶ。また「トラップ」とは、障害が発生した場合に監視ハードウエアから送られる、ハードウエアやソフトウエアの障害箇所を特定するための情報の事である。「トラップ」は、「監視ハードウエア」が持つ変数のアドレスと値を含むデータから構成される。監視ハードウエア１１が不揮発性メモリ上に持つ変数のアドレスと値を含むデータは、トラップとして監視ハードウエア１１からトラップ検知手段１２に送られる。トラップ検知手段１２は、必要に応じて、トラップを検知する。即ち、

自分が知りたい情報以外は無視することもあるが、自分が知りたい情報は取り入れて、トラップを検知する。

【００２８】図１の２０は監視ハードウェア１１から送られてきたトラップ１８の発生順序を保ったままトラップ１８を保管しておくトラップキュー、２１はトラップ検知手段１２が最初のトラップを受信してから電子メールを作成、送信するまでの猶予時間を与えるために時間を計測するタイマーである。

【００２９】次に、動作について説明する。図２は、トラップ検知手段１２がトラップ１８を受信してから電子メール送信手段１４により電子メールを送信するまでの処理を示すフローチャートである。ステップＳＴ１０１において、トラップ検知手段１２は監視ハードウェア１１からトラップを受信するまで待機しており、トラップを受信すると、以下の処理を行なう。ステップＳＴ１０２でトラップ検知手段１２は予め決められたタイマー値でタイマー２１を起動する。タイマー値としては、例えば、何らかの固定値をセットしておけばよい。固定値はプログラムで設定しておいてもよいし、システムのインストール時に設定してもよい。次に、ステップＳＴ１０３でトラップ検知手段１２は、今受信したトラップ１８をトラップキュー２０に追加する。その後、ステップＳＴ１０４にて、イベント待ち状態となり、次のトラップ発生のイベント、またはタイマー満了のイベントを待つ。

【００３０】ステップＳＴ１０４のイベント待ち状態で監視ハードウェア１１から再びトラップを受信する場合の処理の流れを説明する。まず、ステップＳＴ１０５で、イベント発生を検知し、ステップＳＴ１０６でイベントの種類がトラップ発生か、タイマー満了かを判断する。ここでは、イベントの種類がトラップ発生なので、ステップＳＴ１０７でトラップをトラップキュー２０に追加し、再びステップＳＴ１０４に戻り、次のイベントを待つ。トラップ１８を受信する度にこの操作を繰り返し、その都度トラップ１８がトラップキュー２０に追加されていく。

【００３１】次に、タイマー満了の場合の処理の流れを説明する。ステップＳＴ１０４のイベント待ち状態でタイマー２１が満了すると、トラップ検知手段１２は、ステップＳＴ１０８において、電子メール生成手段１３により、トラップキュー２０に蓄えられた全てのトラップ情報を順番に反映した電子メールを作成する。即ち、トラップは、発生順にキューイングされ、キューイングされた順番で電子メール本文に記載される。次に、ステップＳＴ１０９でトラップ検知手段１２はトラップキューをクリアする。最後に、ステップＳＴ１１０において、電子メール送信手段１４により監視者に電子メールを送信する。なお、ステップＳＴ１０９のトラップキュー２０のクリアと、ステップＳＴ１１０の電子メール送信は、順序を入れ替えて実行してもかまわない。

【００３２】なお、監視者に送信される電子メールの内容を図３に示す。発生した時刻の順番でトラップの発生時刻６２、変数アドレス６３、変数値６４が書き込まれている。変数アドレス６３と変数値６４の組み合わせがトラップであり、そのトラップの発生時刻６２とともに電子メールの本文の内容として書かれている。監視者には、トラップ毎の変数アドレスと変数値の組合わせにより、どのような障害、事象が発生したかを示す対応表が別途提供されており、監視者はその対応表と電子メールの内容を照らし合わせることにより、コンピュータにどのような障害、事象が、どのような経緯で発生したかを知ることができる。対応表は、予め提供されているか、あるいは電子メールと並行して提供されているものとする。いずれにしても、電子メール到着時（解析時）に監視者の手元にあればよい。

【００３３】この実施の形態では、監視ハードウエアによりコンピュータの状態を監視し状態情報を保持する機能を有するコンピュータにおいて、発生した障害の内容を電子メールで監視者に通知する際に、障害によるトラップ発生後すぐに電子メールを送信せず、一定時間待ち、その間に検出した複数のトラップをまとめて一つの電子メールで監視者に送信することを特徴とする障害通知方式について説明した。

【００３４】以上のように、この実施の形態によれば、トラップ受信後タイマー猶予時間待ってから電子メールが送られるため、複数のトラップが短い時間内に連続で発生しても電子メールが複数送られることなく、メールサーバ、ネットワークに余計な負荷をかけることが無いという効果が得られる。またトラップキューを用いているため、電子メールに含まれるトラップの発生順序が失われずに監視者に通知され、監視者の解析を容易にする効果が得られる。

【００３５】また、上述した本実施の形態では、猶予時間として予め決めた固定時間を用いているが、それ以外にトラップ受信後の後処理時間を利用することもできる。トラップ受信後の後処理時間とは、トラップを発生させた障害に伴い、コンピュータシステムで行なわれる処理にかかる時間である。ここで、トラップ発生後の後処理とは、データベース停止などコンピュータ上のアプリケーションの緊急停止処理、障害情報の電光掲示板表示、警報ランプ点灯、監視ハードウェアの持つ状態情報のダンプ等のことである。このような時間、例えば、アプリケーションの停止にかかる時間、トラップの発生を電光掲示板に表示する処理にかかる時間、トラップの発生により警報ランプを点灯する処理にかかる時間、監視ハードウエア１１が保持するコンピュータの全状態情報をダンプするためにかかる時間などが、猶予時間として利用できる。これらのトラップ発生後の後処理の時間は、例えば、予め、トラップ検知手段内部など、所定の記憶部に各トラップに対応させて時間を記憶しておき、

検知したトラップに対応する時間をタイマーにセットしてもよい。

【００３６】即ち、この発明の実施の形態の他の例に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、その後処理をする間、電子メールの作成、送信を控え、その間に受信したトラップをキューイングするトラップキューをコンピュータ上に備えたものである。

【００３７】以上のように、この実施の形態の他の例として、上記コンピュータにおいて、障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、トラップ発生後の後処理が完了する間待ち、その間に発生したトラップと一まとめにして一つの電子メールで監視者に送信することを特徴とする障害通知方式について説明した。

【００３８】本実施形態には、さらに次のような改良を加えることができる。ここまで説明した実施例では、タイマーによる猶予時間が固定であったため、以下のような問題がある。まず、障害に関連するトラップの発生が単独で、発生間隔が猶予時間に比べ十分に長い場合、猶予時間待っても待たなくても、メールサーバ、ネットワークにかかる負荷に相違は無く、むしろトラップ発生後猶予時間待つだけ、通知の即時性が失われることとなる。逆にトラップが短時間に連続して発生する場合は、猶予時間待って電子メールを送信しても、その後トラップが続くようであれば、同じ猶予時間後に再度電子メールを送ることになり、このトラップの連続発生を一つの障害、事象として捉えたい監視者に対して、複数のメールに分割されて電子メールが送られ、解析をし難くすることになる。

【００３９】この問題点を解決するために、以下の方法でタイマー２１による猶予時間を動的に変更できるようにする。

【００４０】この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、電子メールを作成、送信するまでの猶予時間を与えるタイマーと、猶予時間内に受信したトラップをキューイングするトラップキューとをコンピュータ上に備え、さらに猶予時間として、前回のトラップ発生からの経過時間に対応する時間、例えば、前回のトラップ発生からの経過時間に反比例する値を動的に決定する、タイマー値決定手段を備えたものである。

【００４１】図４は、図１に示した本実施の形態におけるコンピュータの構成に、トラップを受信した時に前回のトラップ発生からの経過時間をパラメータとして、猶予時間を動的に決定し、決定した猶予時間を用いてタイマー２１を起動することができる、タイマー値決定手段２２を新たに有するものである。また、前回のトラップ発生からの経過時間を求めるために、前回のトラップ発生の時刻を記憶する時刻記憶手段１５を有するものである。これによりトラップの発生がまばらで猶予時間による通知の即時性が失われることが懸念される場合はタイマー値を短くし、逆にトラップが短時間に集中し、猶予時間により電子メールが分割されてしまうことが懸念される場合はタイマー値を長くすることができる。

【００４２】以下に、タイマー値決定の処理の一例について、具体的に述べる。図４に示した構成を採る場合の処理は、図２のフローチャートのステップＳＴ１０２のタイマー起動の処理において、例えば、図５に示すフローチャートで示されるタイマー値決定の処理を行なう。

【００４３】タイマー値決定手段２２がタイマー値を決定する方法について、図５を用いて説明する。ステップＳＴ１１１でトラップが発生すると、ステップＳＴ１１２で時刻記憶手段１５に記憶された前回のトラップ発生時刻と今回発生したトラップの発生時刻から経過時間を計算する。ステップＳＴ１１３でこの経過時間を元に、予め決めておいた固定値パラメータに対し反比例するタイマー値を算出する。例えば経過時間３０分、固定値パラメータを１５（分）とすると、

固定値パラメータ÷経過時間＝タイマー値に従い

１５÷３０＝０．５となり、

次のタイマー値は０．５分となる。

【００４４】ここで経過時間からタイマー値を求めるのに反比例関係を利用する代わりに、両者の合計値が常に一定である関係を利用しても良い。その時の計算式は、

経過時間＋タイマー値＝固定値

となる。

【００４５】このようにタイマー値を決めると、トラップの発生間隔がまばらな間（長い間）はタイマー値が短くなり、トラップの発生間隔が短い場合はタイマー値が長くなるが、場合によってはタイマー値が極端に長くなったり、短くなったりする場合が発生する。経過時間とタイマー値の合計値が一定である関係を利用してタイマー値を設定すると、タイマー値がマイナスになることもあり得る。このような場合の対策として、予めタイマー値の上限値と下限値を設けておき（例えば上限値を５分、下限値を５秒とする）、ステップＳＴ１１４、ステップＳＴ１１５で経過時間から算出されたタイマー値と予め設けられた下限値および上限値との比較を行い、算出されたタイマー値が下限値よりも小さければ下限値を次回のタイマー値として採用する（ステップＳＴ１１８）、算出されたタイマー値が上限値よりも大きければ上限値を次回のタイマー値として採用する（ステップＳＴ１１６）、算出されたタイマー値が両者の間に入っていれば、そのままその値を次回のタイマー値として採用する（ステップＳＴ１１７）ようにする。タイマー値が決まったらステップＳＴ１１９にてタイマーを起動する。

【００４６】このように構成することにより、トラップ

の発生がまばらな間は猶予時間が小さくなり、猶予時間をおくことにより通知の即時性が失われることを防ぐ効果が得られ、逆にトラップが短い時間間隔で連続発生する場合は、猶予時間が長くなり、監視者にメールが分割されて送られ難くなる効果が得られる。

【００４７】以上のように、この実施の形態では、上記コンピュータにおいて、発生した障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、ある一定時間待ち、その間に検出した複数のトラップをまとめて一つの電子メールで監視者に送信する構成において、トラップが発生した際に、前回の障害発生からの経過時間を記録しておき、その時間に反比例する時間を電子メール送信までの待ち時間として採用することを特徴とする障害通知方式について説明した。

【００４８】実施の形態２．これまでに説明した実施の形態１では、監視ハードウエア１１からトラップを受信した後、猶予時間を定めて、猶予時間の間のトラップを溜めた後で電子メールを送信する形態としていた。この方法では１通の電子メールで送る事のできるトラップの数に制限はないため、猶予時間の間に来たトラップが多い場合には非常にデータ量の大きな電子メールを送信する事になる。あまりに大きい電子メールは中継するメールサーバをダウンさせる可能性がある。この実施の形態はこの問題を解消するものである。

【００４９】この実施の形態におけるシステム全体の構成は、従来の図２９に示す構成と同じである。この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、電子メールを作成、送信するまでのトラップ回数を数えるカウンタと、猶予時間内に受信したトラップをキューイングするトラップキューとをコンピュータ上に備えたものである。

【００５０】図６は実施の形態２によるコンピュータの構成を示す図である。図６において、コンピュータの状態を監視し、状態情報を保持する監視ハードウエア１１と、監視ハードウエアからのトラップを受信するトラップ検知手段１２と、受信したトラップを元に電子メールを作成する電子メール生成手段１３と、作成した電子メールを監視者に送信する電子メール送信手段１４とトラップキュー２０は、実施の形態１の図１に示す構成と同じである。図６の３０はトラップの受信のたびに”１”が加算されるカウンタである。カウンタの値は、例えば、トラップ検知手段が保持する上限値と比較される。

【００５１】次に、動作について説明する。図７は、トラップ検知手段１２がトラップを受信してから電子メールを送信するまでの処理を示すフローチャートである。ステップＳＴ１２０において、トラップ検知手段１２は監視ハードウェア１１からトラップを受ける。ステップＳＴ１２１でカウンタ３０を”１”で初期化し、ステップＳＴ１２２で今受信したトラップをトラップキュー２０に追加する。その後、ステップＳＴ１２３にてトラップ発生のイベントを待つ。

【００５２】ステップＳＴ１２３でトラップを受信するとステップＳＴ１２４でトラップをトラップキュー２０に追加する、そして、ステップＳＴ１２５でカウンタ３０に”１”を加える。そして、ステップＳＴ１２６でカウンタ３０が上限値を超えたかどうかを判断して超えていない場合には、ステップＳＴ１２３の処理に戻りトラップ発生のイベントを待機する。

【００５３】ステップＳＴ１２６でカウンタ３０が上限値を超えた場合には、ステップＳＴ１２７において電子メール生成手段１３はトラップキュー２０に蓄えられた全てのトラップ情報を順番に反映した電子メールを作成し、ステップＳＴ１２８でトラップキューをクリアする。最後にステップＳＴ１２９において、電子メール送信手段１４が監視者に電子メールを送信する。そして、ステップＳＴ１２０に戻りトラップ検知手段１２が再びトラップを受信するまで待機する。

【００５４】以上のようにこの実施の形態２によれば、トラップが一定の数たまってから電子メールが送られるため、１通の電子メールに含まれるトラップの数は一定の数になり、多くのトラップを含む、極端にデータ量の大きなメールにより中継するメールサーバをダウンさせる危険を防ぐ事ができる。また、１つのトラップごとに電子メールを送信せず、複数のトラップがまとめて送信されるためメールサーバ、ネットワークに余計な負荷をかけることが無いという効果が得られる。またトラップキューを用いているため、電子メールに含まれるトラップの発生順序が失われずに監視者に通知され、監視者の解析を容易にする効果が得られる。送信される電子メールの内容は図３に示すものと同じである。

【００５５】以上のように、この実施の形態では、上記コンピュータにおいて、障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、トラップの数が一定の個数溜まってから複数のトラップをまとめて一つの電子メールで監視者に送信することを特徴とする障害通知方式について説明した。

【００５６】また、実施の形態２はさらに以下の改良を加える事ができる。ここまで説明した実施例では、トラップの数が上限に達するまで電子メールを送信する事がないため、トラップの数が上限より少ない数で治まる障害が発生するといつまでも障害通報の電子メールが送信されない。これを防ぐために上限を低くすると、多くのトラップが発生する障害が発生した場合に、電子メールの数が増加して、メールサーバ、ネットワークへの負荷が増大し、また１つの障害が複数の電子メールに分割される数が多くなるため解析が難しくなるという問題点が生ずる。

【００５７】この問題点を解決するために、トラップの

数を数えるカウンタの他に、一定の猶予時間経過後には電子メールを送信するためのタイマーを加えた構成を考える。

【００５８】この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、電子メールを作成、送信するまでの猶予時間を与えるタイマーと、電子メールを作成、送信するまでのトラップ回数を数えるカウンタと、猶予時間内に受信したトラップをキューイングするトラップキューとをコンピュータ上に備えたものである。

【００５９】図８は、図６の実施の形態２におけるコンピュータの構成に、タイマー２１を新たに有するものである。これにより、トラップの数が上限に達していなくても、猶予時間の経過後には電子メールが送信されて、上限より少ないトラップが発生する障害の場合にも猶予時間経過後には電子メールを送信する事ができる。

【００６０】次に、図８に示す障害通知方式の動作について説明する。図９は、図８において、トラップ検知手段１２がトラップを受信してから電子メールを送信するまでの処理を示すフローチャートである。ステップＳＴ１３０において、トラップ検知手段１２は監視ハードウェア１１からトラップを受ける。ステップＳＴ１３１でトラップ検知手段１２は予め決められたタイマー値でタイマー２１を起動し、ステップＳＴ１３２でカウンタ３０を”１”で初期化し、ステップＳＴ１３３で今受信したトラップをトラップキュー２０に追加する。その後、ステップＳＴ１３４にてトラップ発生のイベントまたはタイマー満了のイベントを待機する。

【００６１】ステップＳＴ１３４のイベント待ち状態で監視ハードウェア１１から再びトラップを受信する場合の処理の流れを説明する。まず、ステップＳＴ１３４で、イベント発生を検知し、ステップＳＴ１３５で、イベントの種類がトラップ発生か、タイマー満了かを判断する。ここでは、イベントがトラップ発生なので、ステップＳＴ１３６でトラップをトラップキュー２０に追加し、ステップＳＴ１３７でカウンタ３０に”１”を加える。そして、ステップＳＴ１３８でカウンタ３０が上限を超えたかどうかを判断する。超えていない場合には、Ｎｏとなり、ステップＳＴ１３４に戻りトラップ発生、または、タイマー満了のイベントを待機する。

【００６２】ステップＳＴ１３４、ＳＴ１３５のイベント待ち状態でタイマーが満了した場合、あるいは、監視ハードウェア１１から再びトラップを受信して、ステップＳＴ１３７でカウンタ３０に“１”を加えた時にカウンタが上限値に達した場合には、ＳＴ１３８の判断でＹｅｓとなり、ＳＴ１３９で電子メール生成手段により電子メール本文６１が作成される。その後、ステップＳＴ１４０でトラップキューをクリアしてステップＳＴ１４１で電子メール送信手段により電子メールを監視者に送信する。なお、ステップＳＴ１４０のトラップキューのクリアは、ステップＳＴ１４１のメール送信のあとで実行してもよい。

【００６３】この実施の形態によれば、障害通報の電子メールに含まれるトラップの数は上限より多くなる事はないため、極端に大きな電子メールが送信される事がなく、また、トラップの数が上限に達しない場合にも一定の時間の経過後に障害内容をまとめた電子メールを送信できるという効果を得る事ができる。

【００６４】以上のように、この実施の形態では、上記コンピュータにおいて、発生した障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、トラップの数が一定の個数溜まった場合、あるいは、一定の時間経過した場合のいずれかの条件を満たすまでの複数のトラップをまとめて１つの電子メールで監視者に送信する事を特徴とする障害通知方式について説明した。

【００６５】実施の形態３．これまでに説明した実施の形態１、２では、トラップ検知手段１２が、監視ハードウェア１１からトラップを受信した後、そのトラップの内容には関わり無く、猶予時間、あるいはトラップの滞留個数を定義して、ある程度トラップを溜めた後電子メールを送信する形態としていたため、早急に監視者に伝えるべき重大な障害を示すトラップが発生したとしても、ある程度時間が経たなければ電子メールが送られず、監視者への通知が遅れる場合がある。この実施の形態は、この問題を解消するものである。

【００６６】この実施の形態におけるシステム全体の構成は、従来の図２９に示す構成と同じである。この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した時、トラップがその重要度に応じた値を持っており、その値を加算し、合計値がある値に達したら電子メールを作成、送信する障害値加算手段と、加算されている間に受信したトラップをキューイングするトラップキューとをコンピュータ上に備えたものである。

【００６７】図１０は実施の形態３によるコンピュータの構成を示す図である。図１０においても、コンピュータの状態を監視し、状態情報を保持する監視ハードウエア１１と、監視ハードウエアからのトラップを受信するトラップ検知手段１２と、受信したトラップを元に電子メールを作成する電子メール生成手段１３と、作成した電子メールを監視者に送信する電子メール送信手段１４とトラップキュー２０は、実施の形態１の図１、実施の形態２の図６に示す構成と同じである。図１０の４１は、個々のトラップが持つその重大度を示す障害値を加算し、合計値を算出し、算出した合計値を保持する、障害値加算手段である。

【００６８】次に、動作について説明する。図１１は、トラップ検知手段１２がトラップを受信してから電子メ

ールを送信するまでの処理を示すフローチャートである。ステップＳＴ１４２において、トラップ検知手段１２は、監視ハードウェア１１からのトラップ発生を待つ。トラップが発生するとステップＳＴ１４３でトラップ検知手段１２がトラップを検出し、ステップＳＴ１４４でトラップをトラップキュー２０に追加する。次にステップＳＴ１４５において、障害値加算手段４１がトラップの障害値を加算し、合計値を保持する。合計値が予め決められた一定値を越えるまで、トラップが発生する度に以上の処理を繰り返す。ここで、トラップの障害値はその重大度に応じて、例えば”１”から”１０”の１０段階（１０が最も重大な障害を示す）で予めトラップに割り当てられて、例えば、障害値加算手段４１内に保持されているものとする。あるいは、障害値加算手段４１から参照可能であれば、障害値加算手段４１の外部に保持されていてもよい。

【００６９】ステップＳＴ１４６で障害値加算手段４１は、障害値合計が、予め決められた一定値を越えたか判断する。予め決められた一定値を超えると、ステップＳＴ１４７において電子メール生成手段１３がトラップキュー２０に蓄えられた全てのトラップ情報を順番に反映した電子メールを作成し、ステップＳＴ１４８でトラップキュー２０をクリアする。ステップＳＴ１４９で障害値加算手段４１が障害合計値をクリアし、最後にステップＳＴ１５０で電子メール送信手段１４が監視者に電子メールを送信する。送信される電子メールの内容は図３に示すものと同じである。また、ステップＳＴ１４８のキュークリア、ＳＴ１４９の障害合計値クリア、ＳＴ１５０の電子メール送信は、順不同でよい。

【００７０】この実施の形態３によれば、トラップの種類ごとにトラップの重大性、緊急度に応じて重み付けされた値（障害値）を持たせ、その障害値の合計によりメールの送信を判断する。このため、監視者に早く通知すべき重大なトラップが発生すると、その障害値が大きいためすぐに一定値を越えることとなり、監視者に早く通知が行われる効果が得られる。

【００７１】なお、ここでは、障害値を１～１０の１０段階とする例を示したが、１～１００等、他の値でも構わない。また、３段階、５段階など１０より少ない段階にしてもよい。逆に、１５段階、２０段階など、段階を多く設定しても構わない。

【００７２】以上のように、この実施の形態では、上記コンピュータにおいて、障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、トラップの種類毎の重大性、緊急度に応じて、重み付けされた値を持たせ、トラップが発生する度にその値を加算し、合計値が一定の値を越えてから複数のトラップをまとめて一つの電子メールで監視者に送信することを特徴とする障害通知方式について説明した。

【００７３】次に、この実施の形態の変形例について説明する。これまでは、監視者は一人であるという前提の元に、障害通知方式の説明をしてきたが、監視者の中にはローカルなシステム全体の管理を行い、障害が発生する度に処置を行う必要がある情シ部門（情報システム部門）の管理者や、全社のシステムを統合的に管理し、個々の障害に対する処置は行わないが、ローカルシステム毎の障害の発生状況は把握しておく必要がある管理者もいる。後者（以降「全社の管理者」と呼ぶ）は、前者（以降「情シ部門の管理者」と呼ぶ）程の頻度で電子メールが送られる必要は無く、ある程度障害の発生が溜まった段階で電子メールが送られれば十分である。

【００７４】このような要求にも対応するために、本実施形態には、さらに次のような改良を加えることができる。即ち、複数の電子メール送信先を設定することができ、設定先毎に電子メールを作成、送信する障害合計値を変更することができるものである。図１２は、この実施の形態におけるコンピュータの構成を示したものである。図１２は、図１０に新たに５１の送信先テーブルが加わり、トラップキュー２０が送信先テーブルのエントリ数分２０ａ，２０ｂ，．．．２０ｎまで増設されたものである。送信先テーブル５１は監視者の電子メールアドレス５１２と、電子メールを送信する障害合計値５１３、現在の障害合計値５１４を保持するもので、複数のエントリを指定することができる。

【００７５】次に、動作について説明する。図１３は、トラップ検知手段１２がトラップを受信してから電子メールを送信するまでの処理を示すフローチャートである。ステップＳＴ１５１において、トラップ検知手段１２は、監視ハードウェア１１からのトラップ発生を待つ。トラップが発生するとステップＳＴ１５２でトラップ検知手段１２がトラップを受信して検出し、ステップＳＴ１５３でトラップを全てのトラップキュー２０ａ，２０ｂ，．．．２０ｎに追加する。次にステップＳＴ１５４において、障害値加算手段４１が送信先テーブル５１のエントリ毎に現在の障害合計値５１４欄に対応するトラップの障害値を加算し書き込む。ここでエントリ毎に電子メールを送信する障害合計値５１３と現在の障害合計値５１４を比較し（ＳＴ１５５）、現在の障害合計値５１４が電子メールを送信する障害合計値５１３を上回るものが無ければ、再びステップＳＴ１５１に戻り監視ハードウェアからのトラップを待つ。

【００７６】ステップＳＴ１５５で現在の障害合計値５１４が、電子メールを送信する障害合計値５１３を越えるものが検出された場合は、それに該当するエントリ毎に以下の処理を行う（ＳＴ１５６）。ステップＳＴ１５７において、電子メール生成手段１３がエントリに対応するトラップキューのデータを順番に反映した電子メールを作成し、ステップＳＴ１５８で対応するトラップキューをクリアする。ステップＳＴ１５９で障害値加算手段４１がエントリに対応する現在の障害合計値５１４を

クリアし、最後にステップＳＴ１６０で電子メール送信手段１４が監視者に電子メールを送信する。送信される電子メールの内容は図３に示すものと同じである。

【００７７】このように、この実施の形態によれば、監視者（電子メールアドレス）毎に電子メールを送信する障害合計値を変えて登録できる送信先テーブルを設けたので、例えば、障害発生毎に処置の必要な情報システム部門の管理者には早く電子メールが送信され、迅速に処置が行えるようになるとともに、全社の管理者には障害がある程度まとまった段階で適切な頻度で電子メールが送信されるという効果が得られる。

【００７８】以上のように、この実施の形態では、上記コンピュータにおいて、障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、トラップが発生する度に、予めトラップごとに設定してある値を加算し、合計値がある値（予め設定してある送信値）を越えた時に複数のトラップをまとめて一つの電子メールで監視者に送信する際に、送信先によりメールを送信する判断基準となる重み付けされた値の合計値を変化させられることを特徴とする障害通知方式について説明した。

【００７９】実施の形態４．これまでに説明した実施の形態１，２，３ではトラップ検知手段１２が監視ハードウエア１１からトラップを受信した後、ある程度トラップを溜めた後で電子メールを送信する形態としていた。このため重障害が発生した場合は電子メールを送信する前にシステムがダウンする可能性があり、監視者へ通知が行なわれない可能性があった。実施の形態４はこの問題の発生を低減するものである。

【００８０】この実施の形態におけるシステム全体の構成は、従来の図２９に示す構成と同じである。この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、これまでに示した方法である程度障害を溜めてから一つの電子メールで監視者に送信する構成において、コンピュータが短い時間内に停止する可能性のある重障害を示すトラップが発生した場合は、その時の猶予時間、トラップ滞留個数の条件に満たなくとも、電子メールを送信するものである。コンピュータの構成は図１、図４、図６、図８、図１０、図１２の何れかに図１４の５２を加えた構成となる。５２は重障害を示すトラップのテーブル（重障害トラップテーブル）である。

【００８１】次に、動作について説明する。図１５は、トラップ検知手段１２がトラップを受信してから電子メールを送信するまでの処理を示すフローチャートである。ステップＳＴ３０１において、トラップ検知手段１２は、監視ハードウェア１１からのトラップ発生を待つ。トラップが発生するとトラップ検知手段１２がトラップを検出し、ステップＳＴ３０３で検出したトラップが重障害トラップテーブルに存在するかどうか判断する。重障害トラップテーブルに存在する場合、Ｙｅｓとなり、ステップＳＴ３０８で電子メール生成手段１３がエントリに対応するトラップキューのデータを順番に反映した電子メールを作成し、ステップＳＴ３０９で該当するトラップキューをクリアする。最後にステップＳＴ３１０で電子メール送信手段１４が監視者に電子メールを送信する。送信される電子メールの内容は図３に示すものと同じである。この場合、今回発生して検知された（重障害トラップテーブルに存在する）トラップが、電子メールの本文の最後に付くことになり、その前には、そのトラップ以前に、トラップキュー２０にキューイングされていたトラップが並ぶことになる。

【００８２】また、他のメール作成方法として、ステップＳＴ３０８では、今、検出されたトラップ（重障害トラップテーブルに存在するトラップ）だけを電子メール本文に作成してもいい。この場合、ステップＳＴ３０９のキューのクリアは行なわず、まだ、管理者に送信していないトラップを残しておき、次回のメールで送信するようにしてもよい。

【００８３】また、ステップＳＴ３０３の判断で、検出したトラップが重障害トラップテーブルに存在しない場合、Ｎｏとなり、ここでのメール送信は行なわず、ステップＳＴ３０５でトラップキューへの追加処理を行い、再びステップＳＴ３０１に戻り、監視ハードウェアからのトラップを待つ。トラップキューに追加する時の追加処理に付いては、例えば、この実施の形態以外の他の実施の形態で述べているようなトラップのキューへの追加処理を行なうものとする。

【００８４】このように、実施の形態４ではトラップを受信した直後に、重障害を示すトラップのテーブル５２を検索し、トラップのアドレスがテーブル内に存在した場合には、トラップキューの内容を元に電子メール本文を作成して、トラップキューをクリアして電子メールを送信する。

【００８５】このようにする事により、重障害を示すトラップを受信した場合には、すぐに監視者に電子メールが送信され、重障害によるシステムダウンの前に通知できる可能性が高くなる効果が得られる。

【００８６】以上のように、この実施の形態では、上記コンピュータにおいて、発生した障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、これまでに示した方法である程度トラップを溜めてから一つの電子メールで監視者に送信する構成において、コンピュータが短い時間内に停止する可能性がある障害が発生した場合は、電子メール送信待ち時間、滞留個数の条件に満たなくとも、電子メールを送信することを特徴とする障害通知方式について説明した。

【００８７】実施の形態５．これまでに説明した実施の

形態では監視者が複数の場合にも全ての監視者に全てのトラップが送信された。しかし、トラップには、例えば、重度のハードウエア障害を示すトラップ、軽度のハードウエア障害を示すトラップ、ソフトウエアの障害を示すトラップ、停電による無停電電源への切り替えなどシステム障害ではないが環境的な障害に伴って発生するトラップなどいろいろな種類がある。全ての監視者が全てのトラップを監視するのではなく、情報システム部門の管理者はローカルのハードウエア・ソフトウエアのシステム全体を管理するため全てのトラップが必要だが、特定のソフトウエアの管理者はハードウエアの障害は知りたくないがソフトウエアの障害は知りたい、ソフトウエアの障害や停電などのシステムの障害を示さないトラップは必要ないメーカのサポート部門など、監視者により知りたい障害の内容は異なる。

【００８８】このような要求に対応するため、実施の形態５では電子メール送信先ごとにトラップの種類を選別して、その送信先に必要なトラップのみから構成される電子メールの本文を作成して送信する。

【００８９】この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、これまでに示した方法である程度障害を溜めてから一つの電子メールで監視者に送信する構成において、電子メールの送信先ごとに送信するトラップを予め設定したテーブルを持ち、電子メールを作成する時に送信先ごとに、対応するテーブルを検索してテーブルに存在するトラップから構成される電子メールを作成し、電子メールを送信するものである。

【００９０】この実施の形態におけるシステム全体の構成は、従来の図２９に示す構成と同じである。この実施の形態のコンピュータの構成は、図１に示される電子メール生成手段１３を、図１６で置き換えた構成となる。図１６の５４は複数のトラップを選別するための送信トラップ登録テーブルであり、それぞれに番号がついている。この番号は、送信トラップ登録テーブルを識別する識別子の一例である。５３は各電子メールアドレスとトラップを選別するための送信トラップ登録テーブルの対応表（送信トラップ対応テーブル）であり、トラップ種類選別手段６０は送信トラップ対応テーブル５３と送信トラップ登録テーブル５４から、トラップキューにあるトラップのどれをそのメール送信先のためのメール本文に含めるか決定する。そして、電子メール生成手段２３により各電子メールアドレスごとにメール本文が作成される。

【００９１】次に、動作について説明する。図１７はトラップキューの内容を元にして各メール送信先に電子メールを送信するまでの処理を示すフローチャートである。これまでに示した実施の形態におけるメール送信直前の段階で、送信先の各メールアドレスに対してステップＳＴ１６２，ＳＴ１６３，ＳＴ１６４，ＳＴ１６５，ＳＴ１６６で示される処理がそれぞれ行なわれる。

【００９２】ステップＳＴ１６２において送信トラップ対応テーブル５３から送信トラップ登録テーブル５４の番号を求める処理が行なわれる。そして、ステップＳＴ１６３においてトラップ種類選別手段６０によりトラップキューに存在する全てのトラップに対して送信トラップ登録テーブル５４の対応するテーブル番号に存在するトラップが選択されて、選択されたトラップのリストが作成される。ステップＳＴ１６４において選択されたトラップのリストにトラップが存在するかどうか、即ち空でないかどうか判断する。トラップが存在する場合には、ステップＳＴ１６５において選択されたトラップのリストを元に電子メール生成手段２３によりメール本文が作成される。メール本文の内容は図３と同じ内容となる。そして、ステップＳＴ１６６において対応する電子メールアドレスにメールが送信される。トラップが存在しない場合には電子メールを送信しない。そして、次のメールアドレスの処理に戻る。

【００９３】この実施の形態により、各監視者ごとに監視したい障害のみが電子メールで送信され、監視の対象外の障害は送信されず、各監視者が監視の対象となるトラップと対象外のトラップを振り分ける手間が省けるため障害の解析の効率が上がる。また、監視の対象外のトラップはメールに含まれないためメールのサイズは小さくなり、また、監視の対象のトラップがない場合にメールは送信されないため、通信のトラフィックを削減できるという効果が得られる。

【００９４】以上のように、この実施の形態においては、上記コンピュータにおいて、発生した障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、これまでに示した方法である程度トラップを溜めてから一つの電子メールで送信する構成において、監視者の電子メールの送信先ごとに送るべきトラップを設定できる事を特徴とする障害通知方式について説明した。

【００９５】実施の形態６．コンピュータで発生する障害によってはトラップの発生が連続して止まらなくなる場合がある。このような障害が発生すると、トラップに伴う障害の電子メールが監視者に連続して送信される。このためネットワークや途中の中継メールサーバに過大な負荷を与える事になる。この異常な状態はコンピュータがダウンするか、人手によりコンピュータを停止するか、障害を取り除くまで続く。特に夜中など監視者が不在の場合には、対応が遅れて多大な被害が出る可能性がある。実施の形態６はこの問題を解決するものである。

【００９６】この発明の実施の形態に係わる障害通知方式は、トラップの発生が一定の時間間隔以内に起こる状態が一定時間継続したことを検出するトラップ頻発状態検出手段と、逆にトラップが発生しない状態が一定時間

継続したことを検出するトラップ停止状態検出手段とを備え、トラップ頻発状態を検出した際に、電子メールによる障害通知を一時停止するとともに、障害通知を一時停止したことを電子メールで監視者に知らせる、逆にトラップ停止状態を検出した際に、電子メールによる障害通知を再開するとともに、障害通知を再開したことを電子メールで監視者に知らせるものである。

【００９７】この実施の形態におけるシステム全体の構成は、従来の図２９に示す構成と同じである。コンピュータの構成は図１に示されるトラップ検知手段１２を、図１８で置き換えた構成となる。図１８のトラップ検知手段１２ａは、状態変数７１の値がＯＮの場合のみトラップを検知して、状態変数７１の値がＯＦＦの場合にはトラップを検知しない。トラップ検知の停止・再開を制御するトラップ検知制御手段は、トラップが継続しているかを示す状態変数７２と、継続状態を数えるカウンタ７３と、設定されたタイマー値で定期的にタイマーイベントを出すタイマー７４と、タイマーの間隔を設定するタイマー値設定手段７５から構成される。図１９は、この実施の形態におけるタイマー、カウンタの動作を制御する定数値を示す図である。これらの定数値は、図１８の定数値記憶部７７に保持される。

【００９８】次に、トラップ検知の停止・再開を制御するトラップ検知制御手段７０の動作について説明する。図２０，図２１はトラップ検知制御手段の状態遷移図である。初期化の段階でＳ１７０にてカウンタ７３が”０”にセットされて、状態がＳ１７９の中のＳ１７１に移行する。同時にタイマー間隔が図１９のＴｒａｐＵｎｉｔＴｉｍｅに設定されタイマー７４が開始する。この時、状態変数７２は”０”、状態変数７１は”ＯＮ”となる。状態Ｓ１７１においてトラップイベントが発生した場合には、状態Ｓ１７２のトラップが継続している状態に移行し、状態変数７２が”１”になる。この状態でさらにトラップイベントが発生すると状態は移行せずＳ１７２のままとなる。タイマー７４によるタイマーイベントが発生するとＳ１７５でカウンタ７３の値が”１”増加してＳ１７１の状態に戻る。状態Ｓ１７１においてタイマーイベントを受信すると、Ｓ１７４によりカウンタ７３が”０”に設定されて再びＳ１７１に戻る。

【００９９】トラップの発生が長時間継続すると、状態遷移はＳ１７１→Ｓ１７２、ＴｒａｐＵｎｉｔＴｉｍｅの時間経過後にＳ１７２→Ｓ１７５→Ｓ１７１を繰り返し、カウンタ７３の値はその度に”１”増加する。状態Ｓ１７２においてタイマーイベントを受信すると、Ｓ１７４によりカウンタ７３が”０”に設定されて再びＳ１７１に戻る。Ｓ１７５においてカウンタ７３が図１８に示したＴｒａｐＭａｘＣｏｕｎｔに達すると、Ｓ１７９→Ｓ１７７→Ｓ１７３の状態遷移が起こる。この時、状態変数７１が”ＯＮ”→”ＯＦＦ”に変化してトラップの検知を行なわない状態になる。Ｓ１７７でトラップを停止した事がトラップ検知手段１２ａに通知される。トラップ検知手段１２ａは、トラップの検知を停止したことを監視者に電子メールで送信する。トラップの検知を停止した事が電子メールで送信されて、タイマー値設定手段７５によりタイマー間隔がＴｒａｐＲｅｓｕｍｅＴｉｍｅに変更される。

【０１００】状態Ｓ１７３においては、トラップイベントが発生すると、状態遷移Ｓ１７３→Ｓ１７８→Ｓ１７３が発生して、Ｓ１７８でタイマーの残り時間がＴｒａｐＲｅｓｕｍｅＴｉｍｅに戻される。従って、トラップイベントが発生する間隔がＴｒａｐＲｅｓｕｍｅＴｉｍｅより大きくならないとタイマーイベントが発生しない。

【０１０１】状態Ｓ１７３において、トラップの発生が治まってＴｒａｐＲｅｓｕｍｅＴｉｍｅの時間が経過すると、タイマーイベントが発生して、状態遷移Ｓ１７３→Ｓ１７６→Ｓ１７１が発生する。この時Ｓ１７６においてトラップ再開がトラップ検出手段１２ａに通知される。トラップ検出手段１２ａは、トラップの検出を再開した事を電子メールで送信する。トラップの検出を再開した事が電子メールで送信されると、タイマー値設定手段７５によりタイマー間隔がＴｒａｐＵｎｉｔＴｉｍｅに変更される。また、状態変数７１は”ＯＮ”になりトラップの検知を行なう状態を示すようになり、状態変数７２は”０”となる。

【０１０２】このように構成する事により、トラップの発生がＴｒａｐＵｎｉｔＴｉｍｅの時間以内に発生する状態がＴｒａｐＭａｘＣｏｕｎｔ回継続するとトラップの検知が停止される。トラップの発生が止まらなくなる場合にも、約ＴｒａｐＵｎｉｔＴｉｍｅ×ＴｒａｐＭａｘＣｏｕｎｔの時間の経過後にはトラップの検知をやめるため電子メールは送信されなくなり、無限に電子メールが送信される事を防ぐことができる。また、障害の原因が一時的なもので自動的に障害から回復した場合には、ＴｒａｐＲｅｓｕｍｅＴｉｍｅの時間経過後に再びトラップを検知して電子メールを送信できる状態に戻るという効果がある。

【０１０３】以上のように、この実施の形態では、上記コンピュータにおいて、障害によるトラップの発生が一定の時間間隔以内に起こる状態が一定時間継続した際に、電子メールによる障害通報を一時停止し、代わりに監視者には通報を一時停止したことを示す電子メールを送り、その後障害が発生しない状態が一定時間継続した際に、電子メールによる障害通報を再開するとともに、監視者に障害通報を再開したことを示す電子メールを送ることを特徴とする障害通知方式について説明した。

【０１０４】次に、この実施の形態の変形例について説明する。実施の形態６では障害が継続してトラップが止まらなくなると、全てのトラップの検知をやめてしまうため、継続しているトラップ以外の障害が発生しても検

出する事ができないという問題がある。

【０１０５】この問題点を解決するために、トラップ全体の検出を停止するのではなく、継続して発生しているトラップについてのみ検出を停止・再開して、その他のトラップについては影響なく障害の検出を行なう事を考える。

【０１０６】この発明の実施の形態に係わる障害通知方式は、特定のトラップの発生が一定の時間間隔以内に起こる状態が一定時間継続したことを検出するトラップ頻発状態検出手段と、逆に特定のトラップが発生しない状態が一定時間継続したことを検出するトラップ停止状態検出手段とを備え、特定のトラップの頻発状態を検出した際に、電子メールによる特定のトラップの検知を一時停止するとともに、特定のトラップの検知を一時停止したことを電子メールで監視者に知らせる、逆に特定のトラップ停止状態を検出した際に、特定のトラップの検知を再開するとともに、特定のトラップの検知を再開したことを電子メールで監視者に知らせるものである。

【０１０７】図２２は図１７の実施の形態６を各トラップごとに検知の停止・再開を行なえるようにした構成である。各トラップの制御テーブル７６は、各トラップごとについての状態を制御する。制御テーブル７６には障害が継続してトラップが止まらなくなる可能性のあるトラップに対応する、トラップの変数アドレスと、トラップの検知をＯＮ／ＯＦＦする状態と、トラップが継続しているかを示す状態と、トラップが継続している回数を示すカウンタ値と、対応するタイマーの番号が示されている。制御テーブル７６に登録されている各トラップに対応して、７４ａのタイマー０～タイマーｎまでのタイマーがある。トラップ検知手段１２ｂは各トラップの制御テーブル７６に登録されているトラップについて、トラップごとに検知の”ＯＮ／ＯＦＦ”を判断して、トラップを検出する。検知の”ＯＮ／ＯＦＦ”が”ＯＮ”の場合のみ、そのトラップを検知し、検知の”ＯＮ／ＯＦＦ”が”ＯＦＦ”の場合にはそのトラップが発生しても無視する。

【０１０８】次に、動作について述べる。図２３、図２４はトラップ検知制御手段の状態遷移図である。図２５はトラップ検知手段１２ｂのトラップ発生から、トラップの検知、あるいは、無視するまでの判断方法を示したフローチャートである。ステップＳＴ１９０にてトラップが発生すると、ステップＳＴ１９１にてトラップの変数アドレスが各トラップの制御テーブル７６に存在するかどうか検索する。存在しない場合にはステップＳＴ１９５にてトラップを検知する。存在する場合にはステップＳＴ１９３にて制御テーブル７６の検知のＯＮ／ＯＦＦの行のトラップに対応する列を調べる。ＯＮの場合にはトラップを検知する。ＯＦＦの場合にはトラップを検知しない。

【０１０９】トラップ検知の停止・再開を制御する手段の動作は、図２３から図２４の２１の状態遷移図により示される。各トラップの制御テーブル７６に存在する全てのトラップについて、それぞれ、図２３、図２４に示す状態遷移が行われる。状態遷移の方法は図２０と同一であるので詳細な説明は省略する。

【０１１０】このような構成により、制御テーブル７６に存在する特定のトラップの発生が長時間継続した場合に、自動的に特定のトラップに関する電子メールを監視者に送信し続けるのを防ぎ、その他のトラップについては継続して監視できるという効果がある。また、特定のトラップに対する障害が治まった場合に、一定に時間経過後自動的にその特定トラップを監視可能に戻す効果がある。

【０１１１】以上のように、この実施の形態では、上記コンピュータにおいて、あらかじめ登録しておいた特定のトラップを伴う障害の発生が一定の時間間隔以内に発生する状態が一定時間継続した際、その特定のトラップの障害通報を一時停止して、かわりに監視者にはそのトラップに関する通報を停止した事を示す電子メールを送る。なお、その特定のトラップ以外は停止しない。その後、そのトラップの障害が発生しない状態が一定時間継続した際に、電子メールによるそのトラップの通報を再開し、監視者に障害通報を再開したことを示す電子メールを送る事を特徴とする障害通知方式について説明した。

【０１１２】実施の形態７．コンピュータにある障害が発生しても、それが一時的であり短時間内に修復される場合は、障害の発生、修復を示すトラップが短い時間間隔で連続発生する。例を上げると、瞬停（停電後の復電）、ＲＡＩＤ縮退後のホットスペアによる自動再構築開始、などが上げられる。これまでの実施例では、トラップ間の関係には着目しておらず、複数トラップの論理的な区切りを考慮していないため、場合によっては停電発生を示す電子メールが送られた後に、続けて復電を示す電子メールが送られ、監視者は両方のメールを見るまで瞬停であることを判断できないという問題がある。本実施例はこの問題を解決するものである。

【０１１３】この発明の実施の形態に係わる障害通知方式は、コンピュータの運用において、互いに関連があり、比較的短い時間内に連続して発生する可能性の高いトラップの対と、連続発生しなかったと判断できる時間間隔を登録しておく手段を備え、トラップの対の最初のトラップが発生した時に、予め登録した時間待って電子メールを送信し、監視者に知らせるものである。

【０１１４】この実施の形態におけるシステム全体の構成は、従来の図２９に示す構成と同じである。図２６は実施の形態７によるコンピュータの構成を示す図である。図２６においても、コンピュータの状態を監視し、状態情報を保持する監視ハードウエア１１と、監視ハードウエアからのトラップを受信するトラップ検知手段１

２と、受信したトラップを元に電子メールを作成する電子メール生成手段１３と、作成した電子メールを監視者に送信する電子メール送信手段１４と、トラップキュー２０は、実施の形態１の図１に示す構成と同じである。図２３の８０は、互いに関連し連続して発生するトラップの対、例えば、障害トラップと修復トラップの対と、連続発生しなかったと判断する時間間隔を登録しておくトラップ対／時間間隔テーブルである。このトラップ対／時間間隔テーブル８０には、例えば、障害トラップには、”停電”を示すトラップのアドレス、修復トラップには”復電”を示すトラップのアドレス、時間間隔には”１０秒”等の時間を一組としてエントリされる。８１はタイマーで、テーブル８０のエントリ数分ある。

【０１１５】次に、動作について説明する。図２７はトラップ検知手段１２がトラップを受信してから、電子メールを送信するまでの処理を示すフローチャートである。ステップＳＴ２１０で監視ハードウェアからのトラップを待つトラップ検知手段１２が、ステップＳＴ２１１でトラップを受信すると、ステップＳＴ２１２で、まずトラップをトラップキュー２０に追加する。

【０１１６】次に、ステップＳＴ２１３で、トラップ対／時間間隔テーブル８０の障害トラップに受信したトラップと一致するエントリがあるか確認する。なければ、再び、ステップＳＴ２１０でトラップを待つ。ある場合はステップＳＴ２１４で、該当するエントリに登録されている時間間隔で対応するタイマー８１を起動し、ステップＳＴ２１５で対応する修復トラップの発生、またはタイマーの満了を待つ。修復トラップが発生した場合は、ステップＳＴ２１６でＹｅｓとなり、ステップＳＴ２１７で修復トラップを含む電子メールを作成し、ステップＳＴ２１８でトラップキューをクリアした後、ステップＳＴ２１９で電子メールを送信する。修復トラップが発生せず、タイマーが満了した場合はステップＳＴ２２０で障害トラップまでの電子メールを作成し、ステップＳＴ２１８でトラップキューをクリアした後、ステップＳＴ２１９で電子メールを送信する。なお、ステップＳＴ２１８のトラップキュー２０のクリアと、ステップＳＴ２１９の電子メール送信は順序を逆にして処理しても構わない。

【０１１７】このように構成することにより、監視者は一つの電子メールを見ることで、一つのまとまった事象が発生したことを容易に認識することができるという効果が得られる。また障害が短時間内に修復されない場合でも一定時間後に障害情報のみを含んだ電子メールが送られ、障害の発生を見落とすことが無いという効果も得られる。

【０１１８】以上のように、この実施の形態では、上記コンピュータにおいて、あるトラップ発生に対し、比較的短い時間内に続くトラップの発生が予想されるものについて、それらが対で一つの論理的な障害または事象を表す場合は分割せずまとめて一つのメールで通知を行なう事を特徴とする障害通知方式について説明した。

【０１１９】実施の形態８．コンピュータにある障害が発生しても、それが一時的であり短時間内に修復される場合は、コンピュータの運転自体に支障は無く、監視者に通知する必要がない場合がある。例を上げると、ＣＰＵ（Ｃｅｎｔｒａｌ　ＰｒｏｃｅｓｓｉｎｇＵｎｉｔ）使用率が一時的に上限値を越えた場合、メモリ使用量が一時的に上限値を越えた場合、などが上げられる。これまでの実施例では、障害トラップ発生後、その継続時間に着目していないため、短い時間一時的にＣＰＵの使用率が上限値を越えただけでも、監視者に処置する必要の無い電子メールが送られるという問題がある。本実施例はこの問題を解決するものである。

【０１２０】この発明の実施の形態に係わる障害通知方式は、コンピュータの運用において、障害の発生に対し自動的な修復が期待できる事象について、障害トラップと修復トラップの対、および自動修復が望めないと判断できる時間間隔を登録しておく手段を備え、障害トラップが発生した時に、予め登録した時間待っても修復トラップが来ない場合に電子メールを送信し、監視者に知らせるものである。

【０１２１】この実施の形態におけるシステム全体の構成は、従来の図２９に示す構成と同じである。また、コンピュータの構成は実施の形態７の図２６と同じである。ただし、トラップの対の意味と時間間隔の意味が異なる。本実施例においては、図２６の８０は、互いに関連し連続して発生する障害トラップと修復トラップの対と、障害トラップ発生後、自動的な修復がもはや見込めないと判断する時間間隔とを登録しておくテーブルである。８１はタイマーで、テーブル８０のエントリ数分ある。

【０１２２】次に、動作について説明する。図２８は、トラップ検知手段１２がトラップを受信してから、電子メールを送信するまでの処理を示すフローチャートである。ステップＳＴ２３０で監視ハードウェアからのトラップを待つトラップ検知手段１２が、ステップＳＴ２３１でトラップを受信すると、ステップＳＴ２３２で、まずトラップをトラップキュー２０に追加する。

【０１２３】次に、ステップＳＴ２３３で、テーブル８０の障害トラップに受信したトラップと一致するエントリがあるか確認する。なければ、再び、ステップＳＴ２３０でトラップを待つ。ある場合はステップＳＴ２３４で、該当するエントリに登録されている時間間隔で対応するタイマー８１を起動し、ステップＳＴ２３５で対応する修復トラップの発生、またはタイマーの満了を待つ。修復トラップが発生した場合は、ステップＳＴ２３６でＹｅｓとなり、何もせずに再びステップＳＴ２３０でトラップを待つ。修復トラップが発生せず、タイマーが満了した場合は、ステップＳＴ２３７で障害トラップ

を含む電子メールを作成し、ステップＳＴ２３８でトラップキューをクリアした後、ステップＳＴ２３９で電子メールを送信する。なお、ステップＳＴ２３８とステップＳＴ２３９の処理は順序が逆でもよい。

【０１２４】このように構成することにより、監視者は、自動的に復旧し得る障害であって処置する必要の無い、一時的な障害発生を示す不要な電子メールを受信することが無いという効果が得られる。また障害が自動的に復旧し得る障害であっても、一定時間のうちに自動的に復旧せず、処置が必要な場合にのみ電子メールが送られるという効果も得られる。

【０１２５】以上のように、この実施の形態では、上記コンピュータにおいて、ある障害によるトラップ発生に対し、ある程度時間が経てば自動的に修復されることが予想されるものについて、障害が発生してから一定時間に修復されなかった場合に初めて障害とみなして通知を行なう事を特徴とする障害通知方式について説明した。

【０１２６】

【発明の効果】この発明によれば、トラップ受信後、トラップキューにまとめてから電子メールが送られるため、トラップが複数件発生しても電子メールが複数送られることなく、メールサーバ、ネットワークに余計な負荷をかけることが無いという効果が得られる。またトラップキューを用いているため、電子メールに含まれるトラップの発生順序が失われずに監視者に通知され、監視者の解析を容易にする効果がある。

【０１２７】この発明によれば、トラップ受信後タイマー猶予時間待ってから電子メールが送られるため、トラップが短い時間内に連続で発生しても電子メールが複数送られることなく、メールサーバ、ネットワークの負荷を軽減するという効果が得られる。

【０１２８】この発明によれば、トラップ受信後、障害の後処理の完了するまでの間待ってから電子メールが送られるため、トラップが連続で発生しても電子メールが複数送られることなく、メールサーバ、ネットワークの負荷を軽減するという効果が得られる。

【０１２９】この発明によれば、トラップがまばらな間は猶予時間が小さくなり、猶予時間による通知の即時性が失われることを防ぐ効果が得られ、逆にトラップが短い時間間隔で連続発生する場合は、猶予時間が長くなり、監視者にメールが分割されて送られることが発生し難くなる効果がある。

【０１３０】この発明によれば、トラップが一定の数たまってから電子メールが送られるため、１通の電子メールに含まれるトラップの数は一定の数になり、多くのトラップを含む、極端にデータ量の大きなメールにより中継するメールサーバをダウンさせる危険を防ぐ事ができる効果がある。

【０１３１】この発明によれば、障害通報の電子メールに含まれるトラップの数は上限より多くなる事はないため、極端に大きな電子メールが送信される事がなく、また、トラップの数が上限に達しない場合にも一定の時間の経過後に障害内容をまとめた電子メールを送信できるという効果がある。

【０１３２】この発明によれば、監視者に早く通知すべき重大なトラップが発生すると、その障害値が大きいためすぐに一定値を越えることとなり、監視者に早く通知が行われる効果がある。

【０１３３】この発明によれば、監視者毎に電子メールを送信する障害合計値を変えておけば、例えば、障害発生毎に処置の必要な情報システム部門の管理者には早く電子メールが送信され、迅速に処置が行えるようになるとともに、全社の管理者には障害がある程度まとまった段階で適切な頻度で電子メールが送信されるという効果がある。

【０１３４】この発明によれば、重障害を示すトラップを受信した場合には、すぐに監視者に電子メールが送信され、重障害によるシステムダウンの前に通知できる可能性が高くなる効果がある。

【０１３５】この発明によれば、各監視者ごとに監視したい障害のみが電子メールで送信され、監視の対象外の障害は送信されず、各監視者が監視の対象となるトラップと対象外のトラップを振り分ける手間が省けるため障害の解析の効率が上がる。また、監視の対象外のトラップはメールに含まれないためメールのサイズは小さくなり、監視の対象のトラップがない場合にメールは送信されないため通信のトラフィックを削減できるという効果がある。

【０１３６】この発明によれば、トラップの発生が一定の時間以内に発生する状態が一定回継続するとトラップの検知が停止され、トラップの発生が止まらなくなる場合にも、一定の時間の経過後にはトラップの検知をやめるため電子メールは送信されなくなり、無限に電子メールが送信される事を防ぐことができる。

【０１３７】また、この発明によれば、障害の原因が一時的なもので自動的に障害から回復した場合には、一定の時間経過後に再びトラップを検知して電子メールを送信できる状態に戻るという効果がある。

【０１３８】この発明によれば、制御テーブル７６に存在する特定のトラップの発生が長時間継続した場合に、自動的に特定のトラップに関する電子メールを監視者に送信し続けるのを防ぎ、その他のトラップについては継続して監視できるという効果がある。

【０１３９】この発明によれば、監視者は一つの電子メールを見ることで、一つのまとまった事象が発生したことを容易に認識することができるという効果ある。さらに、障害が短時間内に修復されない場合でも一定時間後に障害情報のみを含んだ電子メールが送られ、障害の発生を見落とすことが無いという効果もある。

【０１４０】この発明によれば、監視者は、自動的に復

旧し処置する必要の無い、一時的な障害発生を示す不要な電子メールを受信することが無いという効果がある。さらに、障害が一定時間のうちに自動的に復旧せず、処置が必要な場合にのみ電子メールが送られるという効果もある。

【図面の簡単な説明】

【図１】　この発明の実施の形態１における構成を示す図である。

【図２】　この発明の実施の形態１におけるフローチャートである。

【図３】　この発明の実施の形態１、２、３、４、５、６、７、８における障害の内容を示す電子メール本文である。

【図４】　この発明の実施の形態１において障害が発生した際に前回の障害発生からの経過時間を記録しておき、その時間の逆数に比例する時間を利用する改良を行なう構成を示す図である。

【図５】　この発明の実施の形態１におけるタイマー値決定手段２２のフローチャートである。

【図６】　この発明の実施の形態２におけるトラップの数が制限値に達した場合に電子メールを送信する構成を示す図である。

【図７】　この発明の実施の形態２におけるフローチャートである。

【図８】　この発明の実施の形態２においてトラップの数が制限値に達した、あるいは、タイマーが満了した場合に電子メールを送る改良を行なった構成を示す図である。

【図９】　この発明の実施の形態２においてトラップの数が制限値に達した、あるいは、タイマーが満了した場合に電子メールを送る改良を行なった場合のフローチャートである。

【図１０】　この発明の実施の形態３における構成を示す図である。

【図１１】　この発明の実施の形態３におけるフローチャートである。

【図１２】　この発明の実施の形態３において監視者ごとにメールを送信する障害の重みの合計値を変化させる改良を行なった構成を示す図である。

【図１３】　この発明の実施の形態３において監視者ごとにメールを送信する障害の重みの合計値を変化させる改良を行なった場合のフローチャートである。

【図１４】　この発明の実施の形態４における重障害を示すトラップのテーブルである。

【図１５】　この発明の実施の形態４におけるフローチャートである。

【図１６】　この発明の実施の形態５における電子メール生成手段に相当する構成を示す図である。

【図１７】　この発明の実施の形態５におけるフローチャートである。

【図１８】　この発明の実施の形態６における構成を示す図である。

【図１９】　この発明の実施の形態６におけるタイマー、カウンタの動作を制御する定数値を示す表である。

【図２０】　この発明の実施の形態６におけるトラップ検知の停止・再開を制御する手段の状態遷移図である。

【図２１】　この発明の実施の形態６におけるトラップ検知の停止・再開を制御する手段の状態遷移図である。

【図２２】　この発明の実施の形態６についてトラップが頻発した状態を検知した時に頻発したトラップのみトラップ検知の停止・再開できるように改良した場合の構成を示す図である。

【図２３】　この発明の実施の形態６について各トラップごとにトラップ検知の停止・再開を制御する手段の状態遷移図である。

【図２４】　この発明の実施の形態６について各トラップごとにトラップ検知の停止・再開を制御する手段の状態遷移図である。

【図２５】　この発明の実施の形態６について図２２におけるトラップ検知手段１２ｂのフローチャートである。

【図２６】　この発明の実施の形態７，８における構成を示す図である。

【図２７】　この発明の実施の形態７におけるフローチャートである。

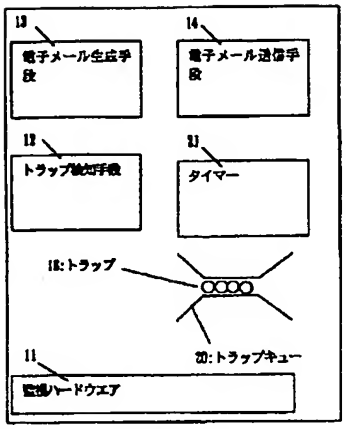
【図２８】　この発明の実施の形態８におけるフローチャートである。

【図２９】　従来の電子メールによる障害通知方式の構成を示す図である。

【符号の説明】

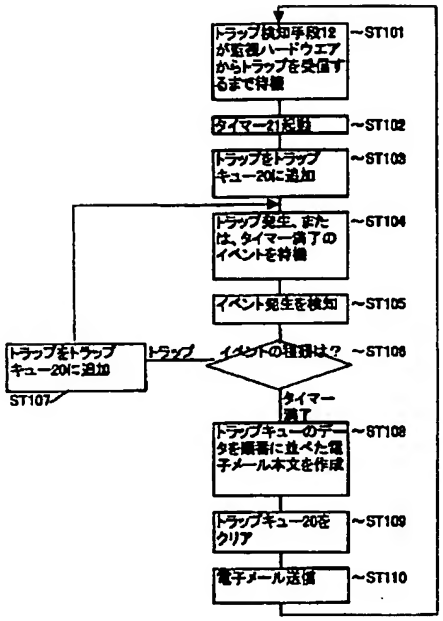
１ａ　コンピュータ（監視対象コンピュータ）、２ａ，２ｂ　メールサーバ、３ａ　管理ＰＣ、４ａ，４ｂ　ＬＡＮ、４ｃ　ＬＡＮ／ＷＡＮ／Ｉｎｔｅｒｎｅｔ、１１　監視ハードウエア、１２，１２ａ，１２ｂ　トラップ検知手段、１３電子メール生成手段、１４　電子メール送信手段、２０，２０ａ，２０ｂ，…２０ｎ－１，２０ｎ　トラップキュー、２１　タイマー、２２　タイマー値決定手段、３０　カウンタ、４１　障害値加算手段、５１　送信先テーブル、５２重障害トラップテーブル、５３　送信トラップ対応テーブル、５４　送信トラップ登録テーブル、６１　電子メールの本文、７０，７０ｂ　トラップ検知制御手段、７１　トラップの検知を行なうか行なわないかを示す状態変数、７２　トラップが継続しているかどうかをしめす状態変数、７３　継続状態を数えるカウンタ、７４，７４ａ　設定されたタイマー値で定期的にイベントを出すタイマー、７５　タイマー値設定手段、８０　トラップ対／時間間隔テーブル、８１　タイマー。

【図１】



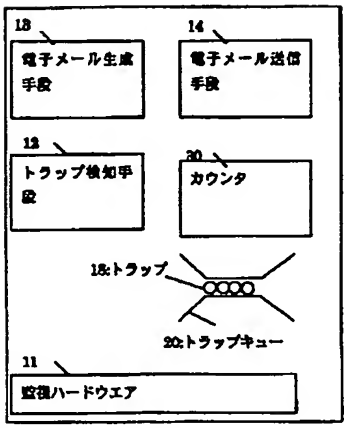
実施の形態１の構成図

【図２】



実施の形態１のフローチャート

【図６】



実施の形態２の構成図

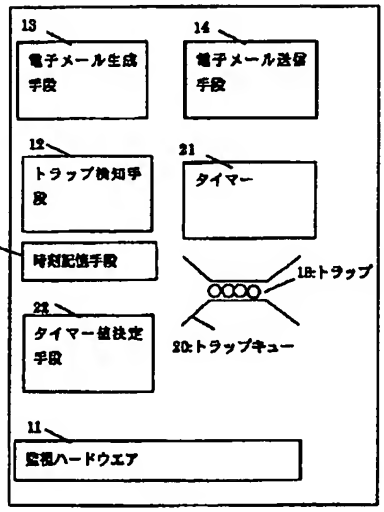
【図３】

61:電子メールの本文

発生時刻 ~62	変数アドレス ~63	変数値 ~64
1999/5/17 20:15:30	0x000A	01
1999/5/17 20:15:31	0x0080	00
1999/5/17 20:15:40	0x0081	10000
1999/5/17 20:15:50	0x007A	00
1999/5/17 20:16:10	0x1002	01
1999/5/17 20:16:11	0x046B	02
1999/5/17 20:16:12	0x05BA	100000

電子メールの本文の内容

【図４】



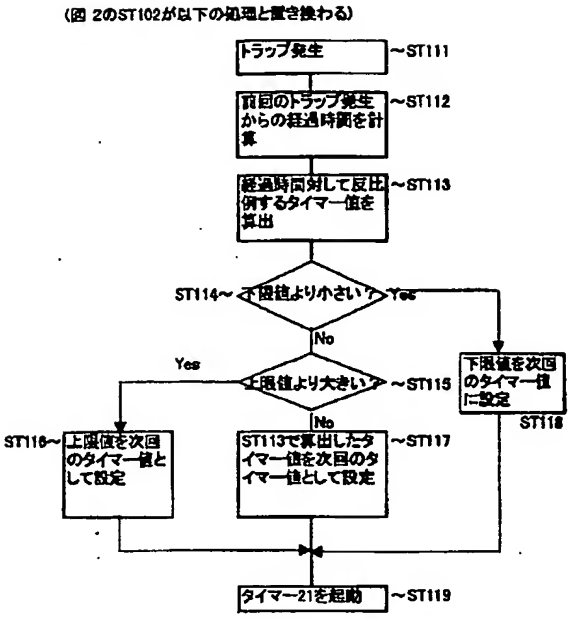
実施の形態１の他の例

【図１４】

52:重障害トラップテーブル

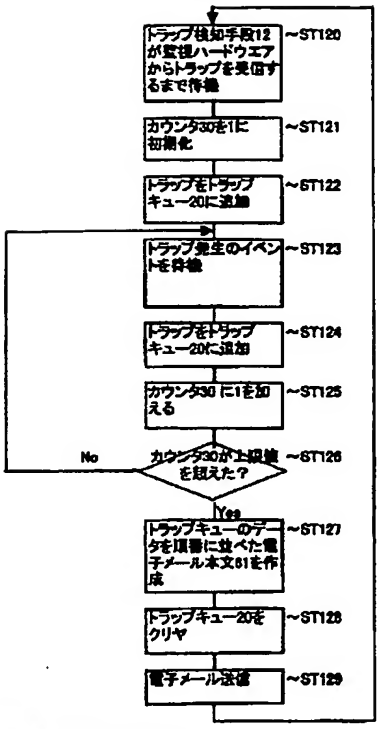
トラップのアドレス
0x0010 ~521
0x0648 ~522
...

【図５】



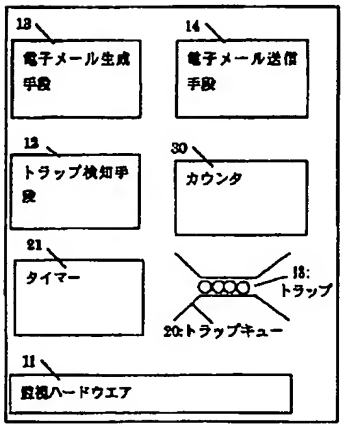
タイマー値決定手段(22)のフローチャート

【図７】



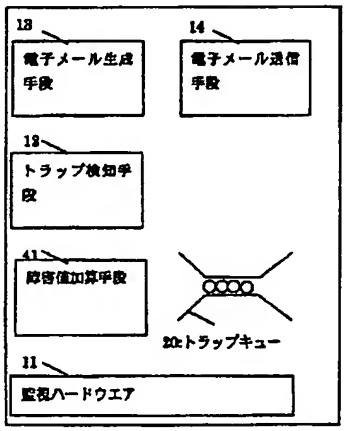
実施の形態2のフローチャート

【図８】



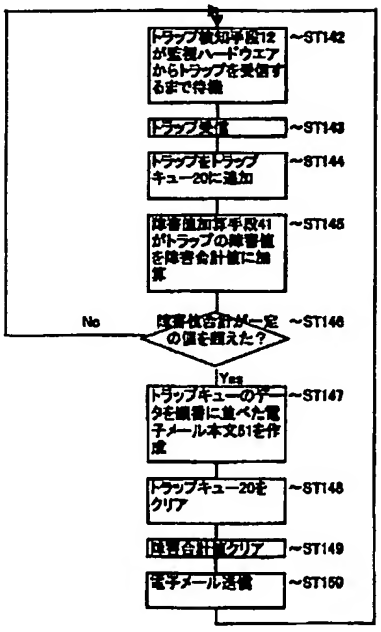
実施の形態2の他の例

【図１０】



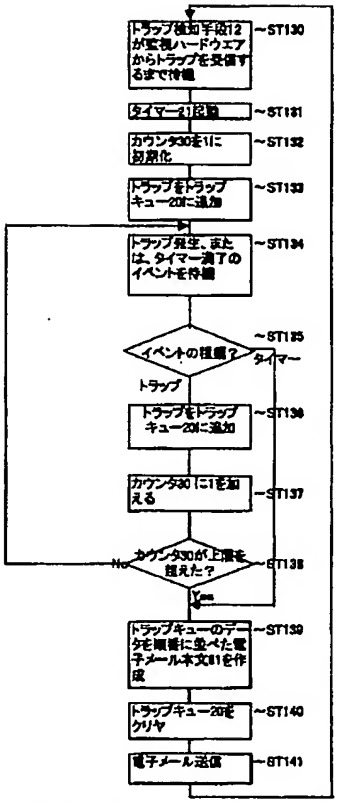
実施の形態3の構成図

【図１１】



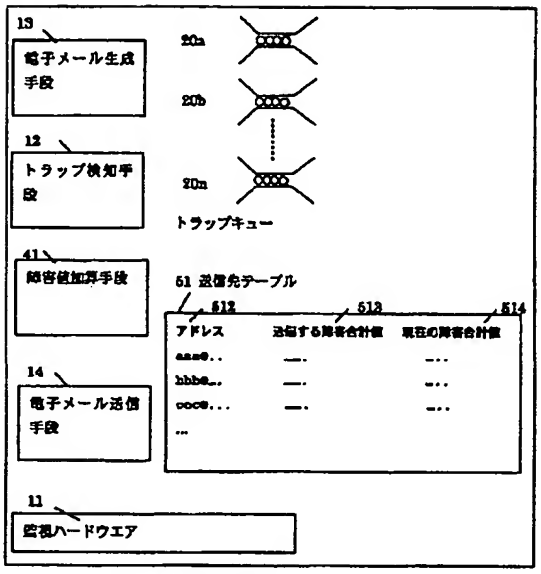
実施の形態3のフローチャート

【図９】



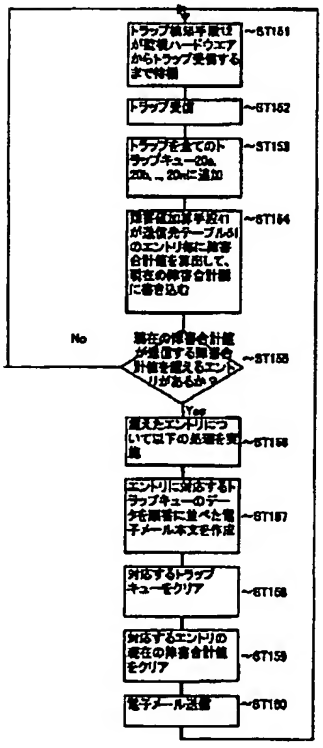
実施の形態2の他の例のフローチャート

【図１２】



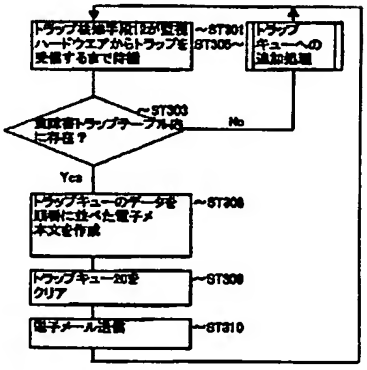
実施の形態３の他の例

【図１３】



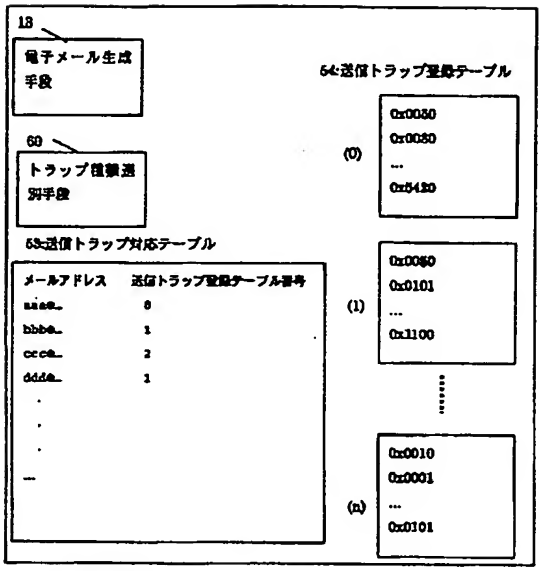
実施の形態３の他の例のフローチャート

【図１５】



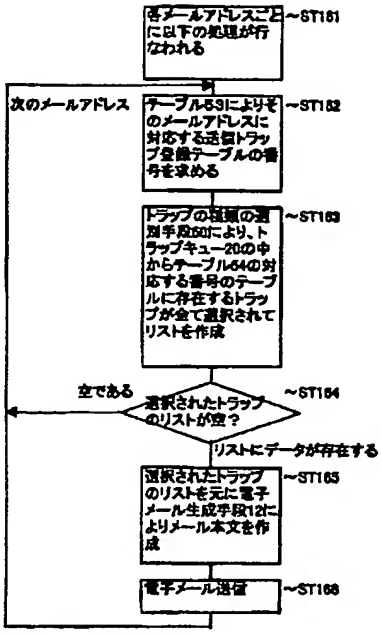
実施の形態4のフローチャート

【図１６】



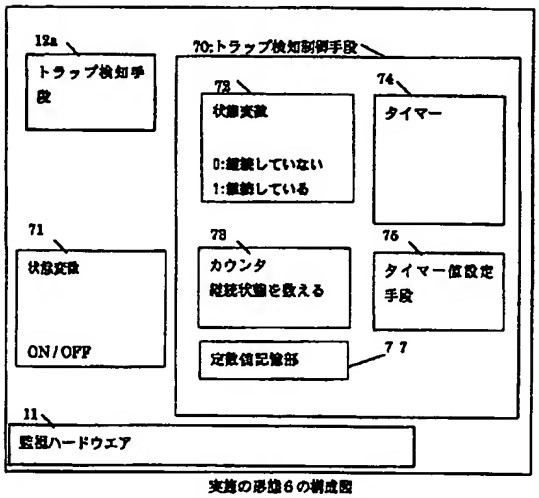
実施の形態５

【図１７】



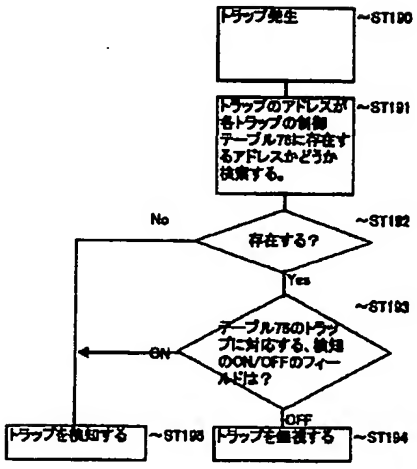
実施の形態５のフローチャート

【図１８】



実施の形態６の構成図

【図２５】



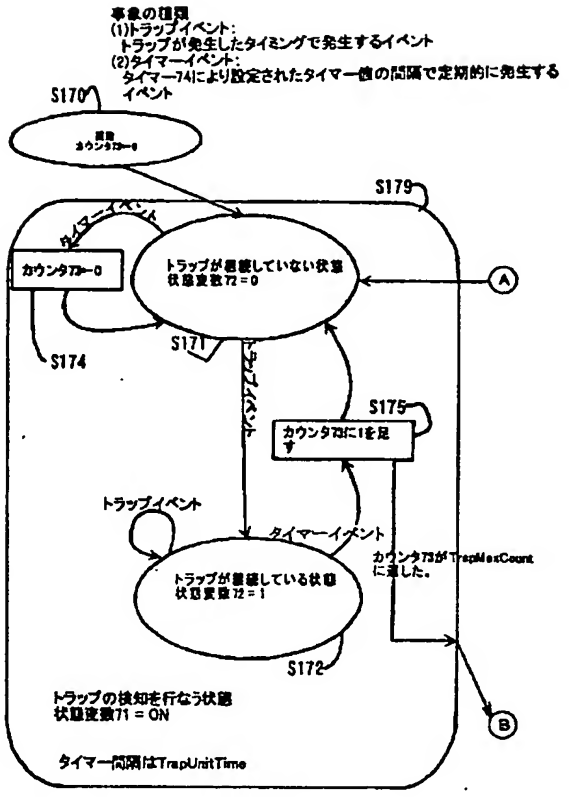
トラップ検知手段12bのフローチャート

【図１９】

TrapUnitTime:	トラップの検知を行なう状態におけるタイマー値
TrapResumeTime:	トラップの検知を行なわない状態におけるタイマー値
TrapMaxCount:	カウンタ 73 の最大値

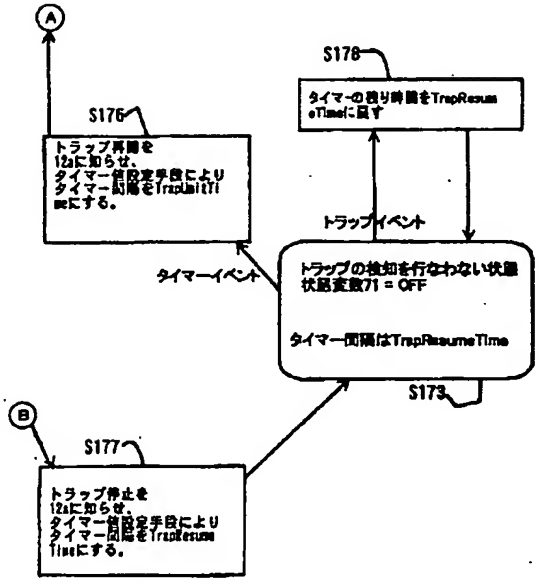
実施の形態６におけるタイマー，カウンタの動作を制御する定数値

【図２０】

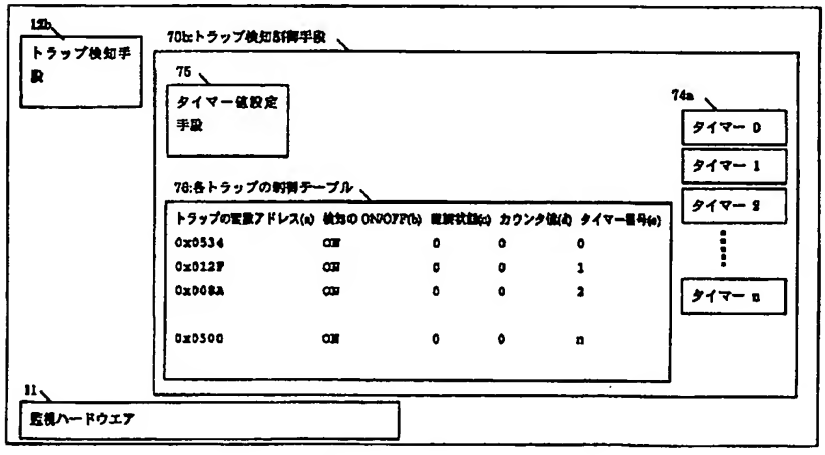


実施の形態６（トラップ検知制御手段の状態遷移図）

【図２１】

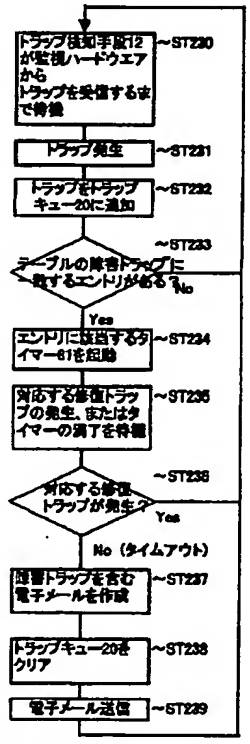


【図２２】



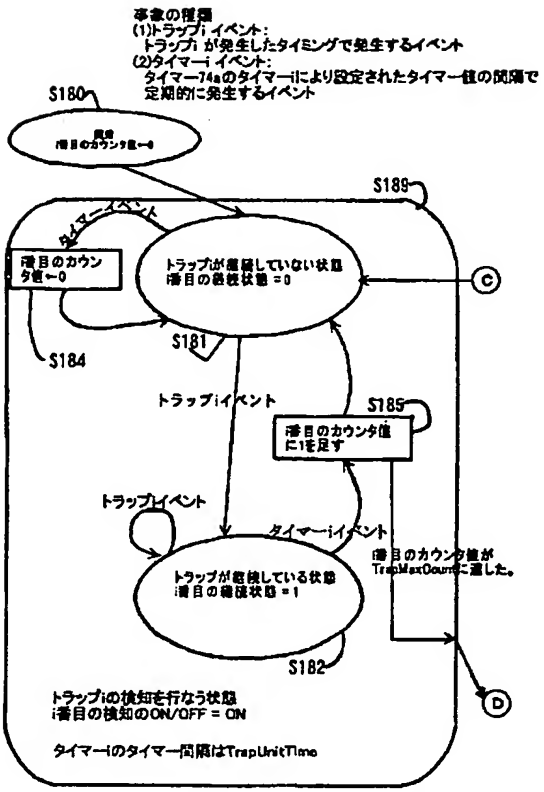
実施の形態６の他の例

【図２８】



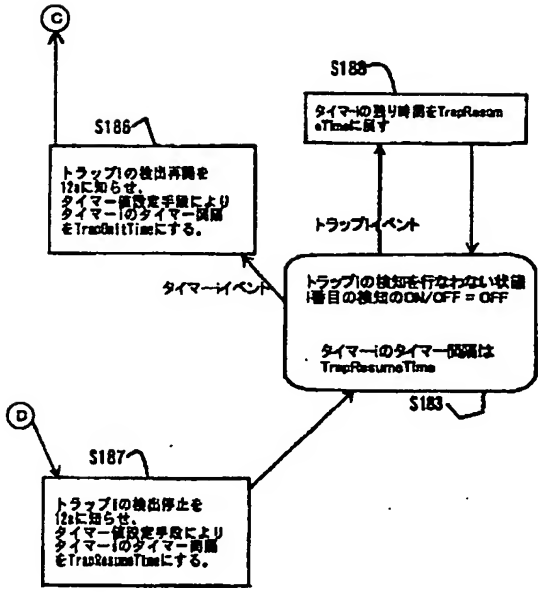
実施の形態６のフローチャート

【図２３】

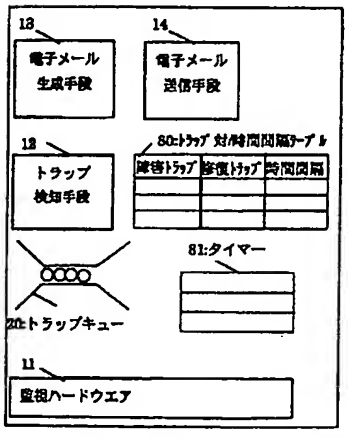


実施の形態６の他の例（トラップ検知制御手段の状態遷移図）

【図２４】

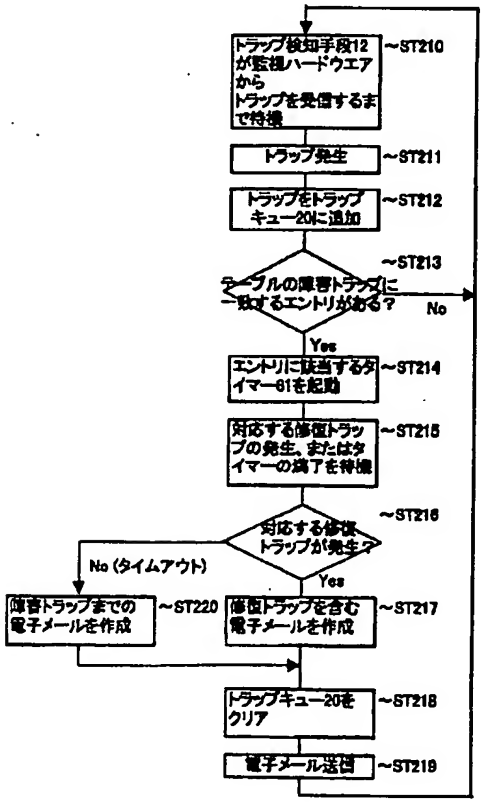


【図２６】



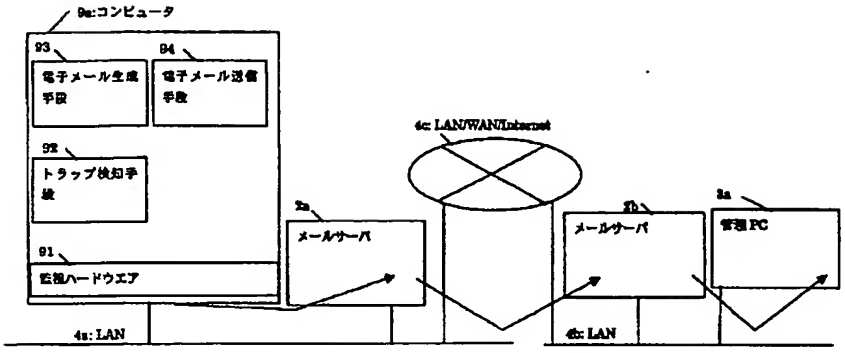
実施の形態７，８の構成図

【図２７】



実施の形態７のフローチャート

【図２９】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/58			

Ｆターム(参考)　5B089 GA23 GB02 JA31 JA35 JB17
KA07 KA12 KC15 KC28 KC29
KC39 LA03 LA06
5K030 GA12 HA06 HB00 JA10 KA21
KX11 MB01
9A001 CC02 CC08 JJ14 JJ25 LL05
LL09